CODES
OF
BUSINESS CONDUCT
AND
ETHICS

KENNETH WIENER
Goodmans LLP, Toronto
kwiener@goodmans.ca

CCCA Annual Meeting
August 2004
CODES OF BUSINESS CONDUCT AND ETHICS

PROPOSED MULTILATERAL POLICY 58-201 – EFFECTIVE CORPORATE GOVERNANCE

- Board should adopt a code of business conduct and ethics for directors, officers and employees of the issuer. Not compulsory – one of the recommended best practices. Code to constitute written standards designed to deter wrong doing and should address:
  - conflicts of interest
  - protection and proper use of corporate assets and opportunities
  - confidentiality of corporate information
  - fair dealing with securityholders, customers, suppliers, competitors and employees
  - compliance with laws, rules and regulations
  - reporting of any illegal or unethical behaviour

- Board should monitor compliance

- Any waivers for directors or senior officers should be granted only by board or board committee

PROPOSED MULTILATERAL POLICY 58-101 – DISCLOSURE OF CORPORATE GOVERNANCE PRACTICES

- If have a code, must be filed on SEDAR no later than filing of annual financials

- Any amendment must be filed on SEDAR within 30 days of board approval

- If waiver granted to officer or director of issuer or subsidiary, must issue and file a news release describing:
  - nature of waiver
  - name of officer or director
  - basis for waiver
  - date of waiver

- AIF must disclosure whether:
  - code adopted and if not, why not
- board monitors compliance and if not, why not
- waiver granted to officer or director during the year and details thereof

NEW YORK STOCK EXCHANGE

- Section 303A.10 of Listed Company Manual – Code of Business Conduct and Ethics
  - Approved by SEC in November, 2003
  - Proposed 58-201 virtual copy of NYSE 303A.10 except NYSE makes code compulsory
  - Differences:
    - NYSE does not include fair dealing with securityholders
    - NYSE requires that code be posted on company’s website

SUMMARY OF CODES

- Schedule “A” is a summary of codes for a sample of 16 of the largest Canadian based TSX-NYSE interlisted companies and U.S. based NYSE companies
- Some codes include topics beyond regulatory requirements
- Focus here on required topics

APPLICATION

- Do you want to go beyond the required directors, officers and employees?
  - Contractors (2/16 in sample)
  - Consultants (6/16)
  - Suppliers (3/16)
  - Agents (1/16)
  - Distributors (2/16)
- Subsidiaries

COMPLIANCE WITH LAWS, RULES AND REGULATIONS

- NYSE specifically refers to insider trading laws
- Three examples in Schedule “B”
• Topics to consider for inclusion (in addition to insider trading):
  ▪ Accounting and financial reporting
  ▪ Trade restrictions and boycotts
  ▪ Environmental laws
  ▪ Responding to litigation and investigations
  ▪ Competition laws
  ▪ Export controls
  ▪ Import regulations
  ▪ Public sector procurement laws
  ▪ Lobbying
  ▪ Anti-bribery laws – conducting foreign business
  ▪ Use of copyrighted materials

• Note the use of examples by GM

CONFLICTS OF INTEREST

• NYSE description:
  ▪ When an individual’s private interests interfere, or appear to interfere, with interests of the corporation as a whole
  ▪ Employee, officer or director takes action or has interests that may make it difficult to perform company work objectively and effectively
  ▪ Employee, officer or director or family member receives improper personal benefits as a result of position in company
  ▪ Loans and guarantees of special concern

• Three examples in Schedule “C”

• Topics to consider for inclusion:
  ▪ Conflict of interest disclosure statement – see Manulife sample form in Schedule “C”
  ▪ Consulting to, or interest in, suppliers
• Kickbacks
• Policy re: giving/accepting gifts and entertainment
• Personal benefits – loans and guarantees
• Hiring family
• Working for competitor
• Outside positions
• Corporate opportunity: duty to the company to advance its interests when opportunity arises
• Soliciting another employee to leave
• Procedure to clear conflicts
  • special procedures for directors?

PROPER USE OF CORPORATE ASSETS
• NYSE description:
  • All employees, officers and directors should protect company’s assets and ensure their efficient use
  • All company assets should be used for legitimate business purposes
• Two examples in Schedule “D”
• Does not replace detailed security policy you probably have
• Topics to consider for inclusion:
  • Funds
  • Books and records
    • adhere to accounting standards
    • transactions properly authorized
    • accurate and complete
  • Physical and intellectual property protection
  • Computer network security
- Personal use of Internet/E-mail
- Review of contracts
- Visible ID

**PROTECTION OF CONFIDENTIAL INFORMATION**

- Two examples in Schedule “E”
- Topics to consider for inclusion:
  - What is confidential information?
    - technical
    - business/financial
  - Guidelines to protect CI
    - non-disclosure agreements with third parties, etc.
  - CI of third parties
- Note “The Code in Real Life” examples by Coca-Cola

**FAIR DEALING WITH OTHERS**

- NYSE description:
  - Each employee, officer and director should endeavor to deal fairly with customers, suppliers, competitors and employees
  - No unfair advantage through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair – dealing practice
- Two examples in Schedule “F”
- Topics to consider for inclusion:
  - Sales practices
  - Treating competitors with respect
  - Reciprocity with suppliers
  - The work environment
- equal employment opportunities
- no work place discrimination or harassment

REPORTING OF ILLEGAL OR UNETHICAL BEHAVIOUR

- Richard Lococo will be discussing reporting systems
- Procedures must be described in your code

EMPLOYEE ACKNOWLEDGEMENTS

- A good idea to require acknowledgement of your code by employees
- Third party acknowledgements if they are included in your code

BILL C-45

- In developing a code, consider implications of the new law on Criminal Liability of Organizations
- Corporation can be convicted of a criminal offence on basis of actions by employees at any level or agents and contractors combined with the intent or negligence of “senior officers”, being anyone who plays an important role in policy making or is responsible for an important aspect of the company’s business
- Code could help address C-45 exposures
SCHEDULES

Schedule “A” – Summary of Codes
Schedule “B” – Compliance with Laws and Regulations: Thomson, GM, IBM
Schedule “C” – Conflicts of Interest: Manulife, AIG, IBM
Schedule “D” – Proper Use of Corporate Assets: Bell, GM
Schedule “E” – Protection of Confidential Information: Nortel, Coca-Cola
Schedule “F” – Fair Dealing with Others: Bell, Thomson
**Summary of Business Conduct and Ethics Codes – Canadian Based TSX-NYSE Interlisted**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>Employees, consultants and suppliers (pg. 3)</td>
<td>Employees, officers, directors of BCE Inc. and subsidiaries, other controlled entities and joint ventures that are not public companies (which have their own codes) (pg. 5)</td>
<td>Employees, officers, directors, contractors and consultants (pg. 1)</td>
<td>Employees, officers and directors</td>
<td>Employees of all RBC companies (Intro)</td>
<td>Employees, officers, directors of Thomson and subsidiaries (Intro)</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Contains principles that are intended to be a guide to making the “right choice”. Identifies the channels and procedures that have been established to answer questions or address concerns (pg. 1)</td>
<td>Lays out minimum standards of conduct that BCE and its Business Units that are not public companies must abide by (pg. 5)</td>
<td>Encana’s Constitution, Corporate Responsibility Policy, Business Conduct and Ethics Practice and related policies are used to identify and manage ethical situations and in making ethical business decisions (pg. 1)</td>
<td>Provides standards for ethical behaviour in representing the Company and when dealing with employees, field representatives, customers, investors, external suppliers, government authorities and the public (pg. 1)</td>
<td>Communicates commitment to highest standards of business conduct and corporate governance; Provides a clear set of expectations and responsibilities (pg. 2)</td>
<td>Eight Guiding Principles to maintain highest standards of honest and ethical behaviour (Our Code of Conduct)</td>
<td>To reaffirm strong commitment to the highest standards of legal and ethical conduct in business practices (pg. 2)</td>
</tr>
<tr>
<td><strong>Consequences for Violation of Code</strong></td>
<td>Compliance with the Code: disciplinary action up to and including dismissal (pg. 16)</td>
<td>Penalties for Violation: disciplinary action up to and including dismissal (pg. 7)</td>
<td>Reference to Investigations Practice</td>
<td>Discipline and/or termination; prosecution if prohibited by law (pg. 2)</td>
<td>Our Responsibilities: “appropriate action” if violated (pg. 6)</td>
<td>Corrective/ disciplinary action; dismissal (Introduction)</td>
<td>Disciplinary Action for Code Violators: possible termination; legal proceedings (pg. 24)</td>
</tr>
<tr>
<td><strong>Reporting of any Illegal or Unethical Behaviour</strong></td>
<td>Compliance with the Code (pg. 16)</td>
<td>Our Responsibility: Business Conduct Help Line (not anonymous) (pg. 6)</td>
<td>Investigations Practice</td>
<td>Reporting Accounting and Auditing Complaints/Concerns (pg. 3)</td>
<td>Our Responsibilities - Where to Go for More Information and Guidance (pg. 5)</td>
<td>Reporting of Irregularities and Dishonesty (Principle 5: Honouring Trust in You)</td>
<td>Investigate and Report any Accounting, Auditing or Disclosure Concerns (pg. 10)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Identify and Report: Fraud, Theft and Illegal or Unethical Behaviour (pg. 17, 18)</td>
<td>Report A Concern: advice line for anonymous reports (pg. 24)</td>
<td></td>
<td>How to Report Concerns &amp; Violations: anonymous phoneline (pg. 25)</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------</td>
<td>----------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliance with Laws and Regulations</td>
<td>International Business (pg. 12)</td>
<td>Our Responsibility (pg. 5)</td>
<td>Compliance with Laws and Regulations (Business Ethics Practice)</td>
<td>Know and Comply with the Law (pg. 17)</td>
<td>We Are Honest and Obey All Applicable Laws (pg. 12)</td>
<td>Principle 1: Upholding the Law</td>
<td>Compliance with Laws, Rules and Regulations (pg. 18)</td>
</tr>
<tr>
<td>Statement of Values</td>
<td>(pg. 1)</td>
<td>Principles of Business (pg. 5)</td>
<td>Corporate Constitution – Our Shared Principles (pg. 8)</td>
<td>Living Manulife Financial’s Values (pg. 4)</td>
<td>Living the Values (Integrity means...) (pg. 6.7)</td>
<td>Eight Guiding Principles (Principle 7: Integrity)</td>
<td>Integrity of Employees (pg. 2)</td>
</tr>
<tr>
<td>Conflicts of Interest</td>
<td>Conflicts of Interest; Loans, Gifts and Entertainment; Family and Personal Relationships; Business Partner-Funded Incentive Programs; Corporate Opportunities; Outside Employment (pg. 7-10)</td>
<td>Conflicts of Interest; Corporate Opportunities; Inducements and Gifts; (Business Ethics Practice)</td>
<td>Deal at Arm’s Length with Suppliers; Bribery and Kickbacks; Gifts; Personal Benefits; Hiring Family Policy; Ethical Investing (pg. 16)</td>
<td>Conflicts of Interest (pg. 12, 16,17,18)</td>
<td>Principle 6: Objectivity (Payments, Gifts, Entertainment; Conflicts of Interest, Directorships)</td>
<td>Conflicts of Interest and Corporate Opportunities; Board Seats on Other Companies (pg. 6)</td>
<td>Gifts, Meals Services and Entertainment (pg. 22)</td>
</tr>
<tr>
<td>Proper Use of Corporate Assets</td>
<td>Employee Use of Company Property (pg. 9)</td>
<td>Safeguarding Company Assets (pg. 16,17)</td>
<td>Protection and Proper Use of Encana’s Assets (Business Ethics Practice)</td>
<td>Protect the Company’s Name and Assets; Use Communications Systems Only for Business; Manage Assets Properly;</td>
<td>Asset Protection (pg. 12)</td>
<td>Misappropriation; E-mail/Internet Use (Principle 5: Honouring our Trust in You)</td>
<td>Protecting Company Assets and Resources (pg. 4)</td>
</tr>
<tr>
<td></td>
<td>E-mail and Internet Usage (pg. 8)</td>
<td>IS/IT Network Security Property; IP (pg. 18)</td>
<td>Protect Personal and Confidential Information (pg. 14)</td>
<td>(pg. 12, 16, 17)</td>
<td>Personal Use of Company Network (pg. 13)</td>
<td></td>
<td>Use of E-mail/Internet, etc. (pg. 5)</td>
</tr>
<tr>
<td>Protection of Confidential Information</td>
<td>Confidential Information and Intellectual Property (pg. 6)</td>
<td>Confidentiality, Business Partner Privacy; Proprietary Information (pg. 12-13)</td>
<td>Confidentiality and Disclosure (Business Ethics Practice)</td>
<td>Confidential Information (pg. 14)</td>
<td>Confidential Information (pg. 14)</td>
<td>Principle 2: Confidentiality</td>
<td>Confidential Information (pg. 8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Refer Media Questions to Communications Departments (pg. 9)</td>
<td></td>
<td></td>
<td>Media, Public and Governmental Inquiries (pg. 12)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Marketing and Sales (pg. 12)</td>
<td>A Work Environment Based on Trust and Respect; Employment Equity (pg. 20, 21)</td>
<td></td>
<td></td>
<td>We Treat Others With Dignity and Respect (pg. 11)</td>
<td></td>
<td>Fair Competition (pg. 23)</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Corporate Responsibility</td>
<td>Environment (pg. 9)</td>
<td>Protecting the Environment (pg. 24)</td>
<td>Human Rights; Labour Practices; Environment; Socio-Economic and Community Development (Corporate Responsibility Policy)</td>
<td>Take Care in Government and Political Dealings; Share Information Responsibly with Government Groups. (pg. 8)</td>
<td>Community Involvement; Political Participation (pg. 22, 23)</td>
<td>Political Contributions, Social and Environmental Responsibility (Principle 4: Corporate Responsibility)</td>
<td>Political Conduct and Contributions (pg. 13)</td>
</tr>
<tr>
<td>Workplace Safety</td>
<td>Health and Safety (pg. 9, 16)</td>
<td>Occupational Health and Safety (pg. 22)</td>
<td>Health and Safety (Corporate Responsibility Policy)</td>
<td>Health and Safety (pg. 11)</td>
<td>(Principle 1: Upholding the Law)</td>
<td>Safe Working Conditions</td>
<td>Drugs and Alcohol (pg. 17)</td>
</tr>
<tr>
<td></td>
<td>Also - separate policy</td>
<td>Drugs and Alcohol (pg. 23)</td>
<td>Also – Alcohol and Drug Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workplace Violence (pg. 24)</td>
<td>Work Place Violence Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling Information</td>
<td>Books and Records (pg. 4)</td>
<td>Books and Records (pg. 17)</td>
<td>Company Records; Accuracy of Books and Records (Business Ethics Practice)</td>
<td>Follow Disclosure Requirements; Respect Copyright; Keep Full and Accurate Records (pg. 15)</td>
<td>Accurate and Complete Reporting (pg. 20)</td>
<td>Inside Information; Copyright; Integrity of Records (Principle 1: Upholding the Law; Principle 7: Integrity)</td>
<td>Accuracy of Records and Information Reporting (pg. 9)</td>
</tr>
<tr>
<td></td>
<td>Shareholder, Media and Community Relations (pg. 15)</td>
<td></td>
<td>Also - Information Management Policy</td>
<td></td>
<td></td>
<td>Use of Copyrighted Materials (pg. 20)</td>
<td></td>
</tr>
<tr>
<td>Harassment</td>
<td>Sexual Harassment, Workplace Harassment and Violence (pg. 14)</td>
<td>Discrimination and Harassment; Reasonable Accommodation (pg. 21)</td>
<td>Separate Non-Harassment Policy</td>
<td>Separate Policy</td>
<td>Discrimination and Harassment (pg. 13)</td>
<td>(Principle 8: Individual Responsibility)</td>
<td>Discrimination and Harassment (pg. 15)</td>
</tr>
<tr>
<td>Securities Laws and Insider Trading</td>
<td>Securities Laws and Insider Trading (pg. 14)</td>
<td>(pg. 11)</td>
<td>Accounting, Auditing or Disclosure Concerns (Business Ethics Practice)</td>
<td>Separate Policy</td>
<td>Insider Trading (pg. 21)</td>
<td></td>
<td>We Compete Fairly (pg. 8)</td>
</tr>
<tr>
<td>Antitrust</td>
<td>Competition Issues (pg. 5)</td>
<td></td>
<td>We Compete Fairly</td>
<td></td>
<td>Antitrust</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractual Authorization</td>
<td>Contract and Agreement Statements (pg. 18)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Planning</td>
<td>Corporate Security – Emergency Management (pg. 23)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Employees and officers of AIG and subsidiaries (pg. 2) [Separate Code for directors, executive officer and senior financial officers]</td>
<td>Employees, officers, directors, temporary workers, independent contractors and consultants of Citigroup, its subsidiaries and their affiliates (pg. 4)</td>
<td>Employees, officers, directors of Coca-Cola and its subsidiaries (pg. 5)</td>
<td>Employees, officers and directors (pg. 1)</td>
<td>Employees, officers, directors, third party representatives such as consultants, agents and distributors, subsidiaries and controlled affiliates included (pg. 4)</td>
<td>Employees, officers and directors of IBM and its subsidiaries and affiliates (pg. 2)</td>
<td>Employees, officers and directors. (pg. 2)</td>
<td>Employees, officers, directors of Wal-Mart, controlled subsidiaries, third parties including suppliers, consultants, service providers (pg. 2) [Separate Code of Ethics for CEO and senior financial officers]</td>
<td></td>
</tr>
<tr>
<td>Purpose</td>
<td>To help AIG employees preserve integrity by providing guidelines for handling business situations appropriately and ethically. (pg. 1)</td>
<td>The Code outlines the principles, policies and laws that govern the activities of the company, and to which employees and others who work with, or represent us, directly or indirectly, must adhere.</td>
<td>Designed to give a broad and clear understanding of the conduct expected of all employees. (pg. 5)</td>
<td>Foundation policies that express the Corporation’s expectations and define the basis for the worldwide conduct of the businesses of the Corporation. (pg. 1)</td>
<td>Introduction to written polices concerning key risk areas, used to reinforce GE’s commitment to integrity. Tool to identify risk areas that employees may come across in their job and what to do if there is a question or concern about an integrity policy. (pg. 2)</td>
<td>To set the policies and obligations that help guide business conduct around the world. Provide direction in applying these principles in day-to-day situations. (pg. 5)</td>
<td>Provides general guidance for resolving a variety of legal and ethical questions for employees of IBM. (pg. 1,2)</td>
<td>Guide to Company policies and legal requirements that govern how business is conducted around the world. (pg. 2)</td>
<td>Introduces specific principles and policies covering key ethics issues. Identifies risk areas. (pg. 1)</td>
</tr>
<tr>
<td>Consequences for Violation of Code</td>
<td>Failure to Follow Code: disciplinary action up to and including termination; civil or criminal penalties (pg. 17)</td>
<td>Introduction: disciplinary action including termination; civil or criminal penalties (pg. 4)</td>
<td>Some Highlights of the Code (pg. 7)</td>
<td>Disciplinary Actions: reprimand, demotion, loss of increases, suspension, termination (pg. 27)</td>
<td>Unspecified</td>
<td>Penalties for Violation: disciplinary action up to and including termination (pg. 7)</td>
<td>Disciplinary Action: Termination; Civil and Criminal Penalties (pg. 3)</td>
<td>Disciplinary Action: disciplinary action including dismissal (pg. 2)</td>
<td>Colleagues and Compliance: prosecution, termination, loss of incentives, other discipline (pg. 6)</td>
</tr>
<tr>
<td>Reporting of any Illegal or Unethical Behaviour</td>
<td>Reporting Concerns: Help Line for anonymous reports (pg. 18)</td>
<td>Raising Ethical Issues; Responsibilities to Citigroup: Ethics Hotline (can be anonymous) (pg. 5)</td>
<td>Your Responsibilities (pg. 11)</td>
<td>Administration of the Code (pg. 26)</td>
<td>Procedures and Open Door Communication (pg. 22)</td>
<td>When you have an Integrity Concern (pg. 6)</td>
<td>Raising an Integrity Concern: GM Awareness for anonymous reports by phone (pg. 3)</td>
<td>Communications Channels: “Speak Up” program for anonymous reports (pg. 3)</td>
<td>Colleagues and Compliance (pg. 6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------------------------------------</td>
<td>--------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Compliance with Laws and Regulations</td>
<td>Customs, Laws and Regulations (pg. 15)</td>
<td>Introduction (pg. 4)</td>
<td>Your Responsibilities (pg. 8)</td>
<td>Ethics Policy (pg. 3)</td>
<td>GE Code of Conduct (pg. 3)</td>
<td>Personal Integrity (pg. 6, 23,116)</td>
<td>The Core Value of Integrity (pg. 3)</td>
<td>Compliance at Pfizer (pg. 6)</td>
<td>Associate Responsibilities (pg. 2)</td>
</tr>
<tr>
<td>Statement of Values</td>
<td>Executive Summary (pg. 2)</td>
<td>Guiding Principles (pg. 2)</td>
<td>GE Code of Conduct (pg. 3)</td>
<td>Vision Statement and Core Values (pg. 3)</td>
<td></td>
<td>Introduction (pg. 2)</td>
<td>Our Standards (pg. 2)</td>
<td></td>
<td>Three Basic Beliefs; Guiding Ethical Principles (pg. 1)</td>
</tr>
<tr>
<td>Conflicts of Interest</td>
<td>Conflicts of Interest (pg. 4)</td>
<td>Conflicts of Interest (pg. 4)</td>
<td>Conflicts of Interest Policy (pg. 14)</td>
<td>Conflicts of Interest (pg. 26)</td>
<td>Disclosure; Interests in Other Businesses; Supplier Relationships; Charitable Activities and Public Service; Outside Employment (pg. 8, 36)</td>
<td>Conflicts of Interest (pg. 20)</td>
<td></td>
<td>Conflicts of Interest (pg. 25)</td>
<td>Conflicts of Interest (pg. 8)</td>
</tr>
<tr>
<td>Proper Use of Corporate Assets</td>
<td>IT Systems; Intellectual Property (pg. 10, 13)</td>
<td>Protecting Citigroup Assets (pg. 6)</td>
<td>Use of Company Assets Policy (pg. 18)</td>
<td>Corporate Assets Policy (pg. 5)</td>
<td>Protecting GE Assets (pg. 25)</td>
<td>Protecting IBM’s Assets (pg. 4)</td>
<td>Patents, Trademarks, and Copyrights (pg. 22)</td>
<td></td>
<td>Wal-Mart Assets (pg. 12)</td>
</tr>
<tr>
<td>Protection of Confidential Information</td>
<td>Confidentiality, Customer Privacy and Data Security (pg. 12)</td>
<td>Proprietary and Confidential Information (pg. 11-12)</td>
<td>Protecting Information (pg. 24)</td>
<td>Corporate Assets Policy (pg. 25)</td>
<td>Protecting Corporate Property; Internet/E-mail and Voice mail Usage (pg. 10, 47)</td>
<td>Protecting IBM Information and Computer Systems; Proprietary Info. (pg. 5) IBM IP Rights; Trademarks (pg. 6, 13)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality and Trade Secrets (pg. 13)</td>
<td></td>
<td>Protecting GE Assets (pg. 25)</td>
<td>Controllship (pg. 27)</td>
<td>Confidential and Proprietary Information (pg. 11, 50)</td>
<td>Communication with the Media (pg. 52)</td>
<td>Confidential and Proprietary Information (pg. 21)</td>
<td>Confidential Information; Trade Secrets (pg. 9, 10)</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>--------</td>
<td>-----------------</td>
<td>---------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIG</td>
<td>Citigroup Inc.</td>
<td>Fair Dealing with Others</td>
<td>General Electric</td>
<td>Exxon Mobil Corporation</td>
<td>Equal Opportunity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coca-Cola</td>
<td>Working with Consumers and Suppliers</td>
<td>Working with Employees</td>
<td>Equal Employment Opportunity Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Electric</td>
<td>Competing with Suppliers and Fair Treatment</td>
<td>Working with Governments</td>
<td>Supply Quality Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exxon Mobil Corporation</td>
<td>Dealing with Suppliers</td>
<td>Working with Governments</td>
<td>Supply Quality Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Motors</td>
<td>Fair Employment Practices</td>
<td>Working with Governments</td>
<td>Supply Quality Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>Work Environment (pg. 4)</td>
<td>Environmental (pg. 18)</td>
<td>Our Commitment; Supporting the Community</td>
<td>Corporate Activity; Protecting Your Safety</td>
<td>Workplace Safety (pg. 3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pfizer Inc.</td>
<td>Equal Opportunity (pg. 9)</td>
<td>Our Commitment; Environmental (pg. 20)</td>
<td>Good Citizenship; Avoiding Improper Payments; Export Controls; Corporate Activity; Environmental Principles</td>
<td>Internal Auditing; Service and Quality</td>
<td>Health and Safety (pg. 15)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wal-Mart Stores Inc.</td>
<td>Integrity and Respect (pg. 13)</td>
<td>Corporate Responsibility (pg. 8)</td>
<td>Corporate Responsibility; Political Activity; Government Delegations; Political Activity; Corporate Activity; Environmental Principles</td>
<td>Internal Auditing; Service and Quality</td>
<td>Health and Safety (pg. 15)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AIG</td>
<td>Citigroup Inc.</td>
<td>Fair Dealing with Others</td>
<td>General Electric</td>
<td>Exxon Mobil Corporation</td>
<td>Equal Opportunity</td>
<td></td>
</tr>
<tr>
<td>Coca-Cola</td>
<td>Working with Consumers and Suppliers</td>
<td>Working with Employees</td>
<td>Equal Employment Opportunity Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
</tr>
<tr>
<td>General Electric</td>
<td>Competing with Suppliers and Fair Treatment</td>
<td>Working with Governments</td>
<td>Supply Quality Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
</tr>
<tr>
<td>Exxon Mobil Corporation</td>
<td>Dealing with Suppliers</td>
<td>Working with Governments</td>
<td>Supply Quality Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
</tr>
<tr>
<td>General Motors</td>
<td>Fair Employment Practices</td>
<td>Working with Governments</td>
<td>Supply Quality Policy</td>
<td>Integrity in the Workplace</td>
<td>Integrity in the Workplace</td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>Work Environment (pg. 4)</td>
<td>Environmental (pg. 18)</td>
<td>Our Commitment; Supporting the Community</td>
<td>Corporate Activity; Protecting Your Safety</td>
<td>Workplace Safety (pg. 3)</td>
<td></td>
</tr>
<tr>
<td>Pfizer Inc.</td>
<td>Equal Opportunity (pg. 9)</td>
<td>Our Commitment; Environmental (pg. 20)</td>
<td>Good Citizenship; Avoiding Improper Payments; Export Controls; Corporate Activity; Environmental Principles</td>
<td>Internal Auditing; Service and Quality</td>
<td>Health and Safety (pg. 15)</td>
<td></td>
</tr>
<tr>
<td>Wal-Mart Stores Inc.</td>
<td>Integrity and Respect (pg. 13)</td>
<td>Corporate Responsibility (pg. 8)</td>
<td>Corporate Responsibility; Political Activity; Government Delegations; Political Activity; Corporate Activity; Environmental Principles</td>
<td>Internal Auditing; Service and Quality</td>
<td>Health and Safety (pg. 15)</td>
<td></td>
</tr>
</tbody>
</table>

The table above provides a structured overview of the codes and companies mentioned in the document.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Handling Information</td>
<td>Communicating with Regulators and Others (pg. 9)</td>
<td>Accuracy of Records and Reporting (pg. 6)</td>
<td>Financial Records (pg. 16)</td>
<td>Corporate Assets Policy (pg. 5)</td>
<td>Controllership (pg. 27)</td>
<td>Accurate Information, Records and Communications; (pg. 9, 56)</td>
<td>Employee Privacy (pg. 4)</td>
<td>Records, Reporting, and Retaining Information (pg. 19)</td>
<td>Books and Record Keeping (pg. 19)</td>
</tr>
<tr>
<td>Harassment</td>
<td>Non-Discrimination and Non-Harassment (pg. 3)</td>
<td>Discrimination and Harassment (pg. 7)</td>
<td>Harassment in the Workplace Policy (pg. 20)</td>
<td>Fair Employment Practices (pg. 24)</td>
<td>Equal Employment Opportunity (pg. 31)</td>
<td>Work Environment (pg. 3)</td>
<td>Discrimination or Harassment (pg. 29)</td>
<td>Discrimination; Harassment and Inappropriate Conduct (pg. 13)</td>
<td></td>
</tr>
<tr>
<td>Securities Laws and Insider Trading</td>
<td>Trading in Securities (pg. 8)</td>
<td>Insider Trading (pg. 13)</td>
<td>Separate Policy</td>
<td>Insider Trading or Dealing &amp; Stock Tipping (pg. 28)</td>
<td>(pg. 85)</td>
<td>Using Inside Information and Insider Trading (pg. 22)</td>
<td>Inside Information (pg. 24)</td>
<td>Insider Trading (pg. 11)</td>
<td></td>
</tr>
<tr>
<td>Antitrust</td>
<td>Antitrust Compliance (pg. 16)</td>
<td>Separate Policy</td>
<td>Antitrust Policy (pg. 10)</td>
<td>Complying with Competition Laws (pg. 21)</td>
<td>Cooperation with Antitrust Enforcement Agencies; Consequences for Antitrust Violations (pg. 80)</td>
<td>Competition (pg. 16)</td>
<td>Antitrust and Competition Laws (pg. 11)</td>
<td>Antitrust (pg. 19)</td>
<td></td>
</tr>
<tr>
<td>Contractual Authorization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authority to Make IBM Commitments (pg. 8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SCHEDULE "B"

Compliance with Laws and Regulations
Compliance with Laws, Rules and Regulations

Know and comply with all laws, rules and regulations applicable to your job.

As a global company, we are subject to numerous laws, rules and regulations. While we do not expect you to be a legal expert, all of our employees are expected to understand and comply with laws, rules and regulations applicable to their jobs and know when to seek advice from your manager or the Thomson legal department. Any violation of laws, rules or regulations applicable to us could jeopardize our integrity. Fraud, dishonesty or criminal conduct will not be tolerated.

As part of your job responsibilities, you should:

- learn about laws, rules and regulations that affect what you do at the company,
- attend periodic training and seek to keep up on any legal developments, and
- consult with the Thomson legal department if you have any questions about the applicability, existence or interpretation of any law or regulation.

We comply with applicable trade restrictions and boycotts.

Our company must comply with all applicable trade restrictions and boycotts. Boycotts may restrict our ability to ship products or offer services in a particular country.

We comply with environmental laws and regulations that apply to our company.

We seek to abide by all applicable environmental standards in the countries in which we operate. Employees have a responsibility to conduct our operations in a manner that complies with laws and regulations, and which minimizes any adverse effect on the environment. We believe that protecting the environment is an important part of being a good corporate citizen. If your job involves contact with regulated materials or involves you in decisions about them, you should understand how those materials can be safely handled to protect you and your fellow employees from harm.

We must recognize the interests of the places in which we do business - currently over 130 countries. In addition to obeying laws and regulations, employees should also respect the local customs of host countries.

If you find yourself in a position that you believe may violate a law, regulation, this Code or another Thomson policy, you should report the violation or what you believe or suspect is a possible violation. You can report your concerns to a manager, your Human Resources department or the Thomson legal department. You can choose to report confidentially and anonymously, as discussed in the section “Questions & How to Report Concerns & Violations” on page 25 of this Code.
Securities Laws and Insider Trading

Don't trade in Thomson securities if you possess material nonpublic information.

No officer, director or employee of the company or any of its subsidiaries may trade in Thomson securities while in possession of material nonpublic information.

Information about Thomson is "material":
- if publicly known, results in or would reasonably be expected to result in a significant change in the market price or value of any Thomson securities, or
- if there is a substantial likelihood that a reasonable shareholder or investor would consider it important in making a decision to buy, sell or hold Thomson securities.

"Nonpublic" information is information that is not generally available to the investing public, either through a press release, distribution to shareholders or widely reported media coverage. The circulation of rumors, or "talk on the street," even if accurate, is not considered public disclosure.

The most common example of "material nonpublic information" about Thomson is information about its earnings or financial performance that has not yet been publicly disclosed. Other examples of material nonpublic information may include:
- a significant change in business operations, projections or strategic plans,
- a potential merger or acquisition,
- a potential sale of significant assets or subsidiaries,
- the gain or loss of a major supplier, customer or contract,
- the introduction of a new product or service,
- a significant pricing change in products or services,
- a declaration of a stock split, a public or private securities offering by Thomson or a change in its dividend policies or amounts,
- a change in senior management,
- major changes in accounting methods, or
- an actual or threatened major lawsuit.

If you are not sure whether information is material or nonpublic, consult with the Thomson General Counsel for guidance before engaging in any transaction in Thomson securities.

You are also prohibited from disclosing material nonpublic information about Thomson to other persons, such as relatives or friends, who may trade on the basis of the information. Securities laws also prohibit trades made on the basis of these "tips." In addition, you should avoid trading in puts and calls relating to Thomson securities.

Don't trade in the securities of other companies if you possess material nonpublic information.

If you have material information about a company with which Thomson does business that is not known to the investing public, you should not buy or sell securities of that company until the information has become public.

In addition to the restrictions above, Thomson has designated certain persons as "Thomson Insiders" because of their position in the company or their actual or potential access to material financial information. "Thomson Insiders" are subject to additional restrictions in terms of their ability to buy, sell or trade Thomson securities. The Thomson General Counsel will notify you if you are a "Thomson Insider."

For more information on insider trading, you should consult the full text of our insider trading policy. If you do not have access to our corporate intranet, thePoint, you can obtain a copy of it from your Human Resources department.

Q: As part of my job, I've recently learned a lot about one of our customers, whose stock is publicly traded. For example, I found out that the customer's revenues for last year are much higher than what the public is expecting to be announced. Can I buy some of their stock at this time?

A: No. Using nonpublic information to buy or sell securities is a violation of the Code and insider trading laws. If you commit insider trading, you could lose your job and possibly face fines and/or jail time.

Q: I know that I cannot buy or sell Thomson stock based on confidential information that I am aware of, but can I recommend to my friends or relatives to buy our stock?

A: No. This is called "tipping" and it's a violation of insider trading laws.
Protecting Intellectual Property and Use of Copyrighted Materials

Protect all intellectual property owned by Thomson and respect the rights of other companies.

Our brand identity and intellectual property are among our most valuable assets and are essential to maintaining our competitive advantages. These include the Thomson name, logo, inventions, processes, innovations, content and software. It is extremely important that we protect these assets, and honor those of third parties. We are responsible for using basic intellectual property protections (such as copyrights, trademarks, service marks and patents) consistently and appropriately.

You should be aware that:

- any intellectual property that employees create in the performance of their job responsibilities belongs to the company and should always be adequately protected. Also, where permitted by applicable law, intellectual property created by contractors or agents under a contract with us are also the property of the company as a work-for-hire. You are expected to promptly disclose any inventions, discoveries and improvements conceived or made during your employment with the company or that are related to company businesses or activities,

- you are required to execute applications, assignments or other instruments upon the company’s request for applications for, and the attainment of, patents or to otherwise protect the interests of Thomson,

- you should report any unauthorized use of the company’s copyrights, patents, trademarks, service marks or other intellectual property to your manager or the Thomson legal department,

- you should get written permission to use a third party’s copyrights, patents, trademarks, service marks or other intellectual property. If you want or need to use intellectual property that belongs to someone else, we must obtain a license to use the property or purchase the outright ownership of the property,

- you should not make copies of, nor publish any copyright-protected materials until we have obtained written permission from the holder and determined that copying or publishing is legally permitted,

- you should put copyright notices on all Thomson materials, information, products, services and other documents or products intended for public distribution or circulation, and

- you should not copy or distribute software or related documentation without ensuring that the licensing agreement permits copying or distribution.

Some Thomson businesses have groups or departments that oversee our compliance in using rights held by third parties. If you are uncertain whom to contact, please consult with the Thomson legal department.

Q: We came across some interesting information in a public database. Can we include it in one of our products without obtaining a permission or consent?

A: The information might still be subject to IP protection. You should consult with the Thomson legal department, as the answer will likely depend on the facts and circumstances.
Use your best judgment in giving and receiving gifts.

We allow employees to offer or receive business gifts, favors and entertainment within specific guidelines. Gifts given or received should never include cash.

Giving gifts – Most countries where we do business forbid employees from making or participating in making any payments designed to cause or improperly influence the decisions of an individual, a company or a governmental official to act in a way that gives the company or the employee an advantage.

Receiving gifts – You cannot solicit, encourage or actually receive any bribe or other payment, contribution, gift or favor that could influence your or another's decision.

A bribe or improper payment is designed to influence another's behavior and is always prohibited. While what is viewed as a bribe in one country may be expected in another, you are expected to comply with this Code. A bribe could take the form of direct cash payments or other forms of payment, such as:

- kickbacks,
- unexplained rebates, or
- invoices for some disguised expense.

Acceptable business gifts, meals, services or entertainment comply with this Code under the following guidelines if they:

- are relatively infrequent and not excessive in value for someone of your position,
- comply with applicable laws and are consistent with customary business practices,
- would not embarrass the company, the person receiving the gift or the person giving the gift, if publicly disclosed, and
- are never given to, or received from, any government official of the United States, Canada or other country.

In some countries, returning or refusing a gift would be offensive. If this occurs, you should accept the gift on behalf of the company and consult with a manager about how the gift should be treated. If you would like to give or receive any business gift, meals, services or entertainment that do not meet the guidelines discussed above, or if you have any questions, you should consult with the Thomson legal department in advance.

Q: A supplier has invited me out for golf and then to dinner and drinks at a steakhouse. Can I accept his offer?

A: Yes, if the invitation is a common business courtesy, is not excessive, and is intended to improve or strengthen the relationship.

Q: We're looking to establish operations in a new country. A local government official has told us that if we make a payment to him, we'll get the necessary approvals and permits much quicker. What should we do?

A: Notify your manager and consult with the Thomson legal department before you do anything. Most payments to government officials are not permitted. However, if the payment has a legitimate business purpose and is considered to be a facilitating payment, and not a bribe, it may be acceptable depending on the circumstances.

Q: Do all government agencies have the same rules and regulations regarding gifts?

A: No. Rules and regulations differ among federal, state, local and foreign government agencies. Consult with the Thomson legal department if you have any questions.
Fair Competition and Antitrust

Compete and deal fairly with our customers, suppliers and competitors and use caution to avoid violating antitrust and competition laws.

We believe in fair and open competition, and our success depends in part on our ability to offer competitively priced quality products and services. While we compete vigorously, we comply with applicable antitrust and competition laws wherever we do business.

Antitrust or competition law is extremely complex and covers a broad range of conduct that may be declared illegal. Many antitrust or competition laws prohibit making agreements with competitors or customers to limit or restrict competition, or sharing information with competitors or customers that would limit or restrict competition. This information could include discussions or agreements with competitors relating to:

- prices,
- products and services,
- business practices,
- territories,
- bids for new business,
- distribution channels, or
- customer lists.

As a general rule, you should avoid discussing these topics with competitors. If a competitor raises any of these topics, you should interrupt and stop the conversation immediately. If you attend a conference and have informal contact with a competitor, it is always a good idea to limit informal contact to the extent possible and keep a written summary of any discussions that may have taken place. The standards for conspiracy to violate antitrust laws are extremely broad and an unlawful agreement can be found where competitors never met or exchanged words, but did something like share competitive information. Antitrust violations do not have to be proven by written agreements and violations can be inferred from an individual’s or organization’s actions. It’s a good idea to use extreme care when talking with competitors or potential competitors.

Because antitrust or competition law is so complex and varies significantly from country to country, you should consult the Thomson legal department in advance of any planned actions that might be considered anti-competitive.

We also deal fairly with our customers, suppliers and competitors. While comparative marketing and advertising are generally acceptable, employees should not unfairly disparage or criticize competitors’ products or services. While we strive to exceed customers’ expectations, we will only make honest and factual claims about our products, services and businesses that can be substantiated. Employees should also not seek to obtain information about our competitors through unlawful or unethical practices.

Q: I’m planning to attend an industry conference and anticipate that I will meet my “equivalent” at a principal competitor. I’ve heard through the grapevine that we are both planning to bid on a new service contract for Corporation XYZ. Can I speak to him?

A: Maybe. You should speak to the Thomson legal department first before you initiate any conversations with a competitor that may pertain to things like pricing and costs. Even an informal discussion at a conference can be a potential antitrust or competition law violation.
PERSONAL INTEGRITY

General

Some things are meant to be taken personally. And nothing is more fundamental to Winning With Integrity than taking personal responsibility for our actions.

We may often encounter circumstances that carry the risk of serious consequences — legal, personal or business. We work in a complex environment and experience increasingly rapid change. We have many new roles, new relationships, new organizational structures and new laws, regulations, rules and policies. Laws have created situations where a failure to make the right choice not only creates risk for the company, but also for the employee involved.

We also operate in an increasingly complex global marketplace with laws which impact almost every facet of our business. These laws can vary country to country. More and more, courts and agencies are not just finding corporations responsible for improper or illegal business conduct. Employees can be held personally accountable for actions that contributed to the violation. We all are responsible for all aspects of our job performance, whether we are acting individually or as a member of a team. Consequently, regardless of position, organization or competitive environment, we must take responsibility for our conduct on the job just as we do in our personal lives.

GM can be a respected, law-abiding company only if we, as its representatives, act with integrity and respect for the law. We have answered that call in the past, and we can do no less as we confront the challenges that lie ahead. As we exhibit the essential traits of basic integrity — honesty, trustworthiness, respect for the law, and respect for others — GM will continue to earn its good reputation and be held in high esteem by its stakeholders.

Complying With the Law

No GM policy is more basic, important or historic: We must comply with all applicable laws and regulations in all countries where we do business.

In order to comply with the law, we must know the law. For many of us, this means we will need advice or training from experts to understand our responsibilities. The significance of the stakes and the number and complexity of all the laws that affect our business require that compliance issues be addressed by employees who have the necessary training and experience.
PERSONAL INTEGRITY

Common sense, our conscience and good intentions — as necessary and reliable as they might be in helping us decide between right and wrong — are not always enough to help us comply with the law. At a minimum, we must learn enough about the laws that affect what we do to spot potential issues and then follow through to get answers about the right way to proceed. This means that every employee whose day-to-day work is directly affected by particular laws has a responsibility to understand them well enough to recognize problem areas and to know when and where to seek advice.

Complying with laws requires more than knowledge. It requires action. If we think some aspect of the way GM is conducting business may possibly violate a law, we must raise the issue with appropriate leadership or the GM Legal Staff.

The sooner we detect a potential problem and move quickly to correct it, the better off we will be in terms of our reputation and protecting ourselves against possible liabilities and penalties. The worst thing we can do is to ignore or try to cover up a potential problem and allow it to grow more severe over time.

**Litigation and Investigations**

Despite our best efforts to comply with all applicable laws and regulations, there will always be matters of interpretation. Litigation is a fact of life in societies governed by many laws that give a variety of authorities broad investigative powers. So, like other businesses, GM is regularly involved in litigation and other proceedings. Legal documents in various forms (papers, E-mail, etc.) related to these legal matters normally flow through established channels, but there may be occasions where other employees receive these documents.

We should consult immediately with the Legal Staff if, as a representative of GM, we receive any summons, subpoena, inquiry, or other communication from any court, marshal, sheriff, government agent, or from any lawyer for any private party or governmental agency. Before submitting to an interview, answering any questions about GM business, producing any documents, or even responding to any requests made in connection with litigation or an investigation, we should consult with the Legal Staff. This applies to matters in which GM is involved directly, such as an investigation of some aspect of our business or a lawsuit involving a GM product or an incident at a GM facility. It also applies to matters in which GM is involved indirectly, including investigations of suppliers, dealers or competitors.

If we are not certain whether a contact we have received involves these issues, we should seek guidance from leadership or the Legal Staff.
Indemnification

On occasion, even when we have done everything right, our actions on the job can become the subject of a legal proceeding or investigation. In these circumstances, we can incur expenses in defending against the claims or charges brought against us individually.

The law of Delaware, where GM is incorporated, permits GM to pay those expenses and any judgments or fines when we act in good faith and in a manner we reasonably believe to be in, or not opposed to, GM's best interests. In addition, GM can indemnify us in a criminal action or proceeding only if we did not have reasonable cause to believe our conduct was unlawful.

GM's policy is to indemnify employees against expenses (including attorney's fees), judgments, fines, and amounts paid in settlement incurred in connection with those legal proceedings or investigations. In addition, GM may advance legal expenses incurred prior to conclusion of a legal proceeding or investigation. Decisions on advancement of legal expenses are made by the Legal Staff on a case-by-case basis.

Breaches of Trust

A familiarity with the basic principles in this section will help us recognize situations that raise questions about what is right. Specific policies exist to provide us with detailed guidance, and members of various staffs are available to give us advice when needed. Some situations may be clear-cut; others may be less clear. We can all think of warning signs: if a contemplated action is rationalized as "doing whatever it takes" or on the basis that "our competition does it" or "no one will ever know," chances are the action needs to be reconsidered.

Taking Action

When we are in doubt about the right choice, it is our responsibility first to ask ourselves:

- Is it legal?
- Is it consistent with our values and policies?
- How would it look on the front page of the newspaper?

If doubt remains, then it becomes our responsibility to seek guidance about the right thing to do, and to keep asking until we find the answer. Our failure to do so can result in severe personal consequences. Violations of GM's policies can result in disciplinary action, up to and including discharge, as well as the imposition of criminal sanctions on us individually or on GM.
Insider Trading

Trading on Nonpublic Information
The U.S. federal securities laws prohibit each of us from buying or selling the stock of any public company, including but not limited to GM, when we have material, nonpublic information that could affect that company.

"Nonpublic information" consists of information that has not been publicly released. "Material" information is information that a reasonable investor would consider important in deciding to buy, sell or hold a security of a certain company. Material information can be favorable or unfavorable. Some examples of information that could be considered material include:

- Significant changes in sales volumes, market share, production scheduling, product pricing or mix of sales;
- Changes in debt ratings or analyst upgrades or downgrades of a company's credit rating;
- Major business acquisitions, dispositions, or contract awards;
- Material labor negotiations or disputes, including possible strikes; or
- Financial, sales and other significant internal business forecasts.

Whether any particular information could be considered material by a "reasonable" investor depends on the specific circumstances existing at a particular point of time. A major factor in determining whether any information is material is the known or potential impact of that information on the company's financial condition, results of operations, or liquidity. If we wonder whether nonpublic information we have is material, we should err on the side of conservatism and treat the information as if it was material.

It is a crime to purchase or sell a company's security, such as stock, while we possess material, nonpublic information about the company. In addition, under the law we may not pass material, nonpublic information on to others who then trade that company's security. Accordingly, we should not:

- Provide material, nonpublic information to family members, business acquaintances, or friends;
- Recommend to anyone that they buy or sell any company's security while we are in possession of material, nonpublic information, even if we do not disclose the specific information to that person; or
- Disclose material, nonpublic information to any GM employees who do not need to know the information to do their job.
If you provide a “tip” to someone who then buys or sells a GM security, whether or not you trade, both you and the “tippee” can be convicted of insider trading. For these same reasons, you should never discuss material, nonpublic information in public places.

When can we trade GM securities? If you are not a GM officer, you may trade GM securities at any time when you do not have material, nonpublic information. If you possess nonpublic information, you must use your own good judgment to determine whether the nonpublic information you possess is material. The mere perception by your friends or business colleagues that you traded on material, nonpublic information could damage both GM’s and your reputation and expose you to potentially serious consequences. To avoid the perception of insider trading and the risk of second-guessing of your trading by others, who may have the benefit of hindsight, you should be very cautious when deciding whether you possess material, nonpublic information.

If you do not possess material, nonpublic information, but because of the nature of your job you are sensitive to how others might judge your trading in GM securities, the safest time to trade in GM securities is during the “window” period beginning on the third day after earnings are announced and ending on the last business day of the middle month of each quarter. However, even in a “window” period you cannot trade GM securities if you possess material, nonpublic information.

The prohibition on trading while we have material, nonpublic information applies to every public company’s securities, not just GM’s. If a job assignment exposes us to nonpublic information about other companies, such as suppliers or customers, we must be vigilant about ensuring that we do not trade in those companies if we have material, nonpublic information about them. Remember, information that may not be material to GM because of our large size may be material to a supplier or other corporation that does business with GM.

Questions regarding this policy or the definition of material, nonpublic information should be discussed with a supervisor or the GM Legal Staff.
Examples

Example

Chris is an Analyst in GM's Treasurer's Office. She's working on an analysis of GM's future pension costs, and she discovers that because of a simple mistake in subtraction GM has grossly overestimated its future costs and has a surplus of several billion dollars in its pension funds. Chris points this out to her boss, who exclaims, "Boy, the stock market is going to love this!" Chris returns to her desk and calls all her friends, urging them to buy GM stock but not telling them why.

Analysis

Because she knows that the pension funds have a large surplus, Chris is probably in possession of material, nonpublic information. If her boss is correct that the stock market would love the information, that indicates that the reasonable investor would consider the information important in deciding whether to buy GM stock, which means that it is material. The information is not public; Chris's boss may be considering publicly disclosing the information but that has not yet happened. Chris may have violated the federal securities laws even though she has not traded stock or divulged the specific information. While in possession of material, nonpublic information she encouraged others to buy stock; if they do so, she is guilty of insider trading.

Example

Ruth works with troubled suppliers at Worldwide Purchasing and has been trying to assist Broken Arrow Axle, Inc., in finding additional financing. Louise, the Broken Arrow Account Representative at BigBanc, its major financier, tells Ruth that BigBanc has informed Broken Arrow that it will not extend any more credit to Broken Arrow. According to Louise, Broken Arrow has asked BigBanc to reconsider, claiming that it will have to file for bankruptcy if BigBanc does not change its mind. Ruth owns BigBanc stock, which she has been considering selling.

Analysis

The important question here is whether Ruth has material, nonpublic information about BigBanc. If she does, she may not sell her BigBanc stock until the information is publicly disclosed or is no longer material. Is Ruth's information material? That would depend upon how important the information would be to a reasonable investor. For example, it is likely that the information would be material to an investor in Broken Arrow, since BigBanc's position could lead to Broken Arrow's bankruptcy. An investor in BigBanc might or might not regard the Broken Arrow situation as important, depending on a number of circumstances, such as the overall size and financial strength of the bank. Ruth should not trade in BigBanc stock without consulting her supervisor or the GM Legal Staff or both.
Compliance With the Law

Each of us has a responsibility to act legally and ethically. There are consequences both to the Corporation and potentially the employee if these obligations are not fulfilled. GM is committed to complying with all applicable laws wherever it does business. In addition to taking steps to ensure full compliance with laws and our policies, we also want to ensure that every GM transaction or activity avoids even the appearance of impropriety.

GM units are responsible for understanding and complying with applicable environmental laws, regulations and GM policies and standards in the design, manufacture, sale, use and disposal of products. Corrective efforts must be initiated as soon as possible if a noncompliance with laws, regulations or GM policy is detected. The Legal Staff should be promptly informed of noncompliant situations and of the corrective plans and actions.

In the U.S., and worldwide, environmental statutes authorize various agencies to seek administrative, civil, and criminal penalties for violation of statutory or regulatory provisions. Under these statutes, criminal sanctions can be imposed upon both GM and individual employees even in the absence of intent or harm to the environment.

Potential Compliance/Enforcement Issues

The Legal Staff is available to assist in compliance and enforcement matters. They should be contacted immediately upon receipt of a violation notice, intent-to-sue letter, complaint, subpoena, information request, or other potential compliance/enforcement matter. This includes oral as well as written notification of potential actions. Advice from the Legal Staff should be sought before we respond to such notices or contacts. We should draw conclusions about GM's compliance status only after a thorough review of the facts and input by the Legal Staff.

Agency Inspections

Agency inspections periodically occur at our facilities. The facility Environmental Engineer will handle these inspections, involve the appropriate team members and provide all necessary information.
Reporting Requirements

It is our policy to inform in a timely manner those who may be affected by conditions caused by our company that might endanger health, safety, or the environment. GM works closely with local plant communities, including emergency planning committees, to ensure an appropriate response to environmental issues of concern. Additionally, state and federal law require timely reports to government agencies of certain spills. If there is any doubt about whether the facility has discovered a “reportable event,” such as a chemical spill or release into the air, contact your plant Environmental Coordinator who is trained to assess the situation.

Our goal is to report timely and responsibly to the authorities. We will assess the facts and make judgments about whether an event is of such quantity or nature that it should be reported.

Record Keeping

In the U.S., the various environmental statutes contain specific provisions about record-keeping requirements. Other countries may have similar requirements, and additional requirements may be identified in plant permits or Corporate bulletins. These requirements pertain to many types of records, such as manifests, monitoring data and training records.

It is essential that all facilities comply with these requirements, and that all such information be accurate, truthful and complete. Under no circumstances should records be falsified or altered in any way. If addendums are made, they should be clearly identified and dated.

Environmental Audits

The GM Environmental Auditing Program is designed to assess both performance to legal requirements and internal objectives and the adequacy and effectiveness of the structure, processes and practices used to identify and manage environmental risks. Where statutes allow, such audits are undertaken at the request of Legal Staff to gain the benefit of privileged and confidential treatment of audit-related documents. An essential component of the environmental audit process is the development of timely action plans that include specific solutions, accountabilities and completion schedules for all reported deficiencies. Action plans must be developed not only to restore deficient performance, but to improve underlying control processes so as to prevent recurrence.
Communications

Given the nature and complexity of our business, our messages from an environmental standpoint can be easily misconstrued. Consequently, our focus is to demonstrate our commitment through deeds, not words. We try to stress what we have accomplished, not what we say we are going to do.

The environmental communications team will assist in developing appropriate statements and responses to internal and external issues. Any specific question from the media related to any environmental situation should be referred to the appropriate communications person.

Examples

As an aid to understanding how we are to fulfill our commitment to the GM Environmental Principles, several hypothetical situations and explanations of how we should conduct ourselves are provided. Whenever we have the slightest doubt about how to proceed in a given situation, questions should be addressed to our leadership, environmental professionals, or, if more appropriate, to the Legal Staff.

Example

Charles works in the Paint Department, but his job duties do not include any specific environmental responsibilities. He’s aware of an ongoing environmental violation that is not being addressed. Does he have to mention it to anyone?

Analysis

Yes. As a GM employee, Charles has an obligation to report any suspected violation to the appropriate plant personnel. If he feels that the matter still has not been addressed, he should contact leadership or call the GM Awareline. The phone number for your location can be found at http://security.gm.com. The GM Awareline is a 24-hour hotline that employees are encouraged to use to anonymously report illegal actions and those which are contrary to Corporate policy.
Example

Lucy oversees the sale of used equipment, some of which is sent to a scrap dealer. A shipment which included a scrapped welding machine was recently sent out of the country, and Lucy has just learned that this machine may still contain a PCB capacitor which should have been removed prior to export. Lucy has a good relationship with the scrap dealer, and knows that she could visit the site and, if necessary, pull the capacitor herself, thereby avoiding the bureaucratic hassle of an "improper PCB export and disposal." The capacitor would easily fit in her briefcase. Lucy would make sure that it was properly disposed of when she had it back in the U.S. In addition, Lucy knows that she would avoid a probable enforcement action, and save the Corporation money, if she simply handled this situation herself. Should Lucy go get the capacitor?

Analysis

No. Lucy should contact the Legal Staff immediately to explain the situation and ask for guidance on the best way to: (1) investigate the situation; and (2) if the PCB capacitor is found, report it to the appropriate authorities. By "quietly handling the matter" Lucy risks compounding the problem both for the Corporation and herself, personally. Up until the point of her learning that the PBC capacitor stayed in the machine when shipped, the activity could be characterized as a mistake. Lucy's proposed solution, however well-meaning, introduces a new element: intentional conduct. Environmental law is complicated; Lucy would be potentially violating U.S. and other regional laws by bringing the capacitor back into the U.S. In general, a good rule of thumb is that you shouldn't do anything that you wouldn't want to be discovered by the government or the public.

Example

John recently transferred to the service garage of a GM assembly plant, where it has been suggested that he pour used oil down the drain. John, a Mechanic, is aware that this practice is damaging to the environment as well as treatment plants, and is, therefore, not an appropriate means to dispose of used oil. John's supervisor, Sue, has been very busy lately, and he is concerned about bringing yet another issue to her attention. What should he do?

Analysis

The disposal of used oil down a drain is likely to violate regulations, internal GM policy requirements, and good environmental control practice. Such disposal poses a potential hazard to human health and the environment. John should approach Sue with the idea that there may be a better, safer way to dispose of the used oil. John or Sue should contact the local environmental support office to determine if there is an on-site collection location for used oil or if any local gas stations operate as an oil recycling location.
Bringing this concern to Sue's attention is the "the right thing to do." It is also in keeping with GM Environmental Principle #2, "We are committed to reducing wastes and pollutants, conserving resources and recycling materials at every stage of the product life cycle." GM is committed to being a responsible corporate citizen and is working hard to continuously improve its environmental performance. Environmental responsibility is the duty of all GM employees.

Example

Elena, a GM Plant Communications Coordinator, has been asked by the local Rotary Club to give a presentation at its next meeting on environmental stewardship activities in which her plant is involved. Should she accept the invitation? If so, what information should she provide?

Analysis

Elena should first inform her management of the invitation and receive approval to participate in the Rotary Club function. Her acceptance of the invitation falls under GM Environmental Principle #3, "We will continue to participate actively in educating the public regarding environmental conservation." Environmental stewardship is the responsibility of every GM employee. Programs to reach this goal are encouraged at every level.

Elena could gather examples from various departments throughout the plant of activities under way both in the workplace and in the home. Her speech could include descriptions of the following initiatives:

- Programs to recycle office white paper, bottles and cans;
- Programs to reduce paper usage by encouraging two-sided copying;
- Programs to reduce natural resource and energy usage and nonproduct (waste) output;
- Programs to demonstrate innovative new environmental control technologies;
- Requests to employees to power down or turn off lights, computers and copy machines when not in use;
- Programs to encourage employees to become involved in environmental education programs in local schools; and
- Publication of regular notices to employees that include environmental tips, such as the efficiency of regular car tune-ups and planned driving.
Example

Jean's neighbor, Kathy, is active in a local environmental group. Kathy has mentioned that the group hopes to have legislation introduced that would create local industrial water discharge limits. Jean wonders if she should mention the issue to anyone within GM.

Analysis

Jean should discuss this matter with the environmental personnel at her facility. Because Jean has learned about a piece of legislation that has not yet been introduced, this would be an opportunity for GM to work with interested stakeholders and legislators before the bill becomes final. This is in keeping with GM Environmental Principle #5, "We will continue to work with all governmental entities for the development of technically sound and financially responsible environmental laws and regulations."
The core value of integrity

Our business ethics policy reflects a fundamental commitment to integrity and honesty in all business dealings. No one, from the most senior executive to the newest employee, is ever expected to commit or condone an illegal or unethical act, or to instruct other employees to do so. Not in the name of business efficiency. Not to get results. Not for any reason.

We stake our reputation on adherence to the highest of ethical standards, which surpass the letter of the law and embrace open and honest relations with employees, customers, sales associates, shareholders, communities, governments, suppliers and competitors. Our respect for what the law intends and our standards, which seek to surpass the letter of the law, do not mean that, on occasion, there will not be legitimate doubt as to the proper interpretation of the law. Nor does it mean that legal disagreements with other persons will not occur from time to time nor that the company will abandon its legitimate legal defenses or rights.
many instances such a payment would not be lawful. You must get the approval of IBM Governmental Programs and IBM counsel before inviting these speakers.

4.9 Complying with Laws

IBM’s policy is to comply with all laws and regulations that apply to its business. As you conduct IBM’s business, you may encounter a variety of legal issues, particularly in the areas described below. If you have questions on specific laws or regulations, contact IBM counsel.

4.9.1 Competition

Laws governing competition exist in most of the industrialized countries in which IBM does business. The purpose of competition laws, which also may be known as antitrust, monopoly, fair trade or cartel laws, is to prevent interference with the functioning of a competitive market system. While the purpose of such laws is primarily economic, their effect is often seen as going beyond consumer welfare to protecting other values of society, including individual freedoms.

Under these laws, companies may not enter into agreements with other companies, including their distributors and remarketers, however informally, that unreasonably restrict the functioning of the competitive system, such as price fixing or dividing clients or territories.

Companies also may violate competition laws without acting jointly with other companies by, for example, illegally monopolizing or attempting to monopolize an industry or unlawfully abusing a dominant position.

IBM’s policy is to comply fully with competition laws throughout the world. You can help by adhering to all of IBM’s business conduct guidelines, by being sensitive to legal concerns under competition laws, and by raising any such concerns with IBM counsel.

4.9.2 Export

IBM is truly an international business, with relationships in most of the world’s countries and IBM is in a “high technology” industry. As a result, IBM technology in the form of products and services, and all technical data relating to the design, production and use of those products and services is subject to U.S. and foreign export control laws and regulations. That means that when IBM products and technical data are exported, IBM must obtain an export authorization from the U.S. or appropriate foreign government.

You should be aware that your actions may have export implications. Export laws apply to: all international transactions, including international intercompany ones and ones where the recipient is a non-U.S. national inside the U.S.; transactions with clients, suppliers, and original equipment manufacturers; and when we use Business Partners, alliance partners or agents to complete a delivery or provide a service—any relationship where IBM will be involved with the export of commodities, technical data, software, technical assistance and similar support.

Export laws cover more than just physical shipments. Internet and extranet transfers of technology; application development and delivery; e-business and e-services activities; travel outside the United States with IBM products or technology; providing technical specifications and performance requirements to suppliers for procurement from non-U.S. sources; and the
application of personal knowledge (technical assistance) abroad—all involve activities that are subject to U.S. and other country export requirements.

It is against the law to export without authorization or to facilitate the unauthorized export of IBM technology. Penalties for failure to comply with export laws and regulations are severe and can result in fines, loss of export privileges and imprisonment. If you have questions on export-related issues, talk with your manager or your local Export Regulation Coordinator or contact the Export Regulation Office (w3.ibm.com/chq/ero).

4.9.3 Antiboycott

U.S. law prohibits IBM and its subsidiaries and affiliates and their agents from complying with or supporting a foreign country’s boycott of a country which is “friendly” to the United States. IBM is also required to report promptly to the U.S. Government any request to support a boycott or to furnish information concerning a boycott. A foreign country or an entity associated with the country could make such a request in a bid invitation, purchase order or contract, letter of credit or orally in connection with a transaction or in a number of other ways. Examples of improper boycott requests are requests that we refuse to do business with a boycotted country, including its citizens, or with so-called blacklisted companies who do business with the boycotted country or that we provide information about activities in a boycotted country or implement letters of credit with boycott conditions. If you hear of a boycott or receive a request to support a boycott or to provide information related to a boycott, you should contact your manager, IBM counsel or the Export Regulation Office (w3.ibm.com/chq/ero).

4.9.4 Import

As a major importer, IBM must comply with import regulations and requirements when engaging in international trade. Because of the continued globalization of IBM’s business, there are many situations, some of them very subtle, in which your work may have import implications. For example, in addition to the obvious one in which you are importing parts or products into the U.S. or another country, there may be import implications in activities, such as development process activity requiring non-U.S. sourcing, client activity requiring the shipment of parts to another country, the shipment of marketing samples, or the calculation of product intercompany prices for sales to an IBM location in another country. In addition, experience has shown that designing parts and ensuring accuracy of inventory of parts will have import implications whenever those parts will cross international borders. You need to be aware of import regulations and requirements, especially if you are involved in importing. A failure to comply with the law can result in fines, penalties, imprisonment and/or a loss of import privileges. If you have questions about imports, contact your manager, your local Import Requirements Coordinator, the IBM Worldwide Distribution International Trade Compliance organization in Boulder, Colorado or a related IBM Worldwide Distribution organization, or the Import Compliance Office (w3.ibm.com/chq/ico).

4.9.5 The Environment

IBM is committed to worldwide leadership in environmental protection. Not only will we comply with all environmental laws, but if there is no law or if the law does not protect the environment, we will set and adhere to stringent standards of our own. Each of us must comply with environmental laws and IBM’s environmental policies.
If you are involved with processes that affect the environment, such as measuring, recording or reporting discharges and emissions to the environment or handling hazardous wastes, you must be sure to comply with environmental regulations and permits. You must also maintain IBM standards and ensure that reports are accurate and complete.

As an employee, you have a role to play in protecting the environment. If you become aware of any violation of environmental law or any action that may appear to conceal such a violation, you should immediately report the matter to your manager or to IBM counsel.

4.9.6 Public Sector Procurement

The purpose of public sector procurement laws is to help public sector clients, such as federal, state, and local governments and agencies and those who act on the government's behalf, to get the products and services they want at fair and reasonable prices. Since these laws vary widely and some are complex, we must be careful in our public sector procurements to comply fully with those laws. During the course of a public sector procurement, you should not try to improperly influence the decisions of the client or obtain restricted information about the procurement.

The following are some examples of specific issues you should be sensitive to in public sector procurements. Procurement laws generally require competitive bidding and permit sole source procurement only in unique circumstances. You may review an advance copy of a solicitation document only if the client has also made it available to other bidders. You may not prepare a solicitation document on behalf of a public sector client, even at the client's request, or submit any anonymous documents, such as white papers, to a public sector client, or encourage a public sector client to sign an agreement before an award is made to IBM. You should never discuss business or employment opportunities that could personally benefit any public sector procurement personnel, and you must not offer or provide gratuities in connection with a procurement activity. If you plan to use a consultant in a government client procurement situation, you may not hire a consultant without proper authorization from your management and with the involvement of IBM Global Procurement or IBM counsel. You must ensure that such consultants are governed by our business conduct guidelines. You must also not engage any consultant where doing so would create a conflict of interest.

Because we are committed to serve the public trust in accordance with the law, you must understand and adhere to all applicable public sector procurement laws and regulations. Additionally, you should immediately report to IBM any actual or possible violation of a public sector procurement law or regulation. This may be done through your manager, IBM counsel, the IBM Speak Up program or any of IBM’s other communications channels. IBM will not tolerate retaliation against you for making that report and, subject to any applicable business or legal requirements, IBM will protect your anonymity.

4.9.7 Lobbying

Any contact with government personnel for the purpose of influencing legislation or rule making, including such activity in connection with marketing or procurement matters, is considered lobbying. Some laws also define lobbying even more broadly to include our normal marketing activities. You are responsible for knowing and adhering to all the relevant lobbying laws and associated gift laws, if applicable, and for compliance with all reporting requirements.
You must obtain the prior approval of IBM Governmental Programs to lobby or authorize anyone else (for example, a consultant, agent, or Business Partner) to lobby on IBM’s behalf, except when lobbying involves only normal marketing activities and not influencing legislation or rule making.

4.9.8 Accounting and Financial Reporting Laws

As a public company, IBM is required to follow strict accounting principles and standards, to report financial information accurately and completely, and to have appropriate internal controls and processes to ensure that accounting and financial reporting complies with law. Each of us in IBM must comply with these requirements and do what is needed to help IBM, as a company, comply.

The rules for accounting and financial reporting require the proper recording of, and accounting for, revenues and expenses. If you have responsibility for or any involvement in these areas, you must understand and adhere to these rules. Also, these rules prohibit anyone from assisting others to account improperly or make false or misleading financial reports. Therefore, you must accurately and completely record and report all information, and you must not assist anyone to record or report any information inaccurately or in a way that could be misleading. Additionally, you must never provide advice to anyone outside of IBM, including clients, suppliers and business partners, about how they should be recording or reporting their own revenues and expenses.

Violations of laws associated with accounting and financial reporting can result in fines, penalties, and imprisonment, and they can lead to a loss of public faith in a company. If you become aware of any action related to accounting or financial reporting that you believe may be improper, you should immediately tell IBM; this may be done through your management, IBM counsel, IBM Internal Audit or by informing IBM management using any of IBM’s other communications channels. If you wish to report your concerns anonymously, you can use the IBM Speak Up program. If you have any questions, you may contact IBM counsel or IBM Internal Audit.
5.1.5.2 Closely Held Organizations

Investments in closely held organizations—typically, closely held corporations, partnerships or even sole proprietorships—raise additional concerns over those in publicly traded companies because of the closer ties of investors to most closely held organizations. For example, there are generally relatively few investors or owners of such companies, giving each a greater stake in ownership; the investors often have a chance to participate in the company’s day-to-day operations; and the investors may be perceived to be closely identified with the company.

This relatively close relationship may give the appearance to competitors of the closely held organization that it derives some benefit from IBM. Such a relationship may also give the appearance to IBM employees that the investing employee is using IBM’s time, facilities or confidential information for the benefit of the closely held company. For these reasons, employees may not make any investment in a closely held organization that is a competitor, supplier, distributor or organization that remarkets IBM products. Exceptions must be specifically approved by management with the advice of IBM counsel.

5.2 Using Inside Information and Insider Trading

In the course of your employment with IBM, you may become aware of information about IBM or other companies that has not been made public. The use of such nonpublic or “inside” information about IBM or another company for your financial or other benefit not only is unethical, but also may be a violation of law. U.S. law makes it unlawful for any person who has “material” nonpublic information about a company to trade the stock or other securities of the company, including options, puts, calls, and any derivatives or to disclose such information to others who may trade. Violation of such laws may result in civil and criminal penalties, including fines and jail sentences. IBM will not tolerate the improper use of inside information. These prohibitions also apply outside the U.S.

Material inside information is information which is not available to the general public and which could influence a reasonable investor to buy, sell or hold stock or securities. While it is not possible to identify in advance all information that could be viewed as material inside information, some examples might include nonpublic information about: IBM’s financial performance including earnings and dividend actions; acquisitions or other business combinations; divestitures; major new product or services announcements; significant advances in research; and, other significant activities affecting IBM. Here are some examples of how you can avoid the improper use of inside information:

- If you know that IBM is considering an alliance or is about to announce a new product or make a purchasing decision that could affect the price of the securities of an IBM supplier or other company, you should not buy or sell the securities of that company until after the information becomes public.

- Similarly, if you know that IBM is about to make an announcement that could affect the price of its own securities, you should not buy or sell IBM securities on the open market until after the announcement.

- You should not buy or sell the securities of a client or alliance company based on any inside information you have about that company.

- If you have nonpublic information that IBM is about to build a new facility or expand an existing facility, you should not invest in land or in any business near the new site.
You should not disclose inside information to IBM employees who do not have a business need to know or to anyone outside of IBM.

As with investments, you should not evade these guidelines by acting through anyone else or by giving inside information to others for their use even if you will not financially benefit from it.

If you have any doubt about what you can or cannot do in this area, you should consult with IBM counsel.

5.3 Public Service

IBM encourages employees to be active in the civic life of their communities. However, such service may, at times, place you in a situation that poses a conflict of interest with IBM. As a board or committee member, you may, for example, be confronted with a decision involving IBM. It might be a decision to purchase IBM equipment or services; or it might be a decision by a board of tax assessors or a zoning board that affects IBM property. In such circumstances, your interest in IBM and your obligation to the civic organization might pull you in opposite directions. The law may require you to abstain, depending on your position in IBM and whether you stand to gain personally from the decision. On the other hand, there may be circumstances in which the law does not permit you to abstain. While you are in the best position to make the decision and bear the responsibility for the decision, before making your decision, you should get advice from the civic organization’s lawyer and from IBM counsel. In order to protect IBM from embarrassment or other issues, whether or not you finally abstain, you should make it clear that you are an IBM employee and thereby head off any charges of trying to conceal your association with IBM. And, if you decide to abstain, state clearly that you are doing so because there would be a conflict of interest—or the appearance of one—if you did not.

5.4 Participation in Political Life

IBM will not make contributions or payments or otherwise give any endorsement of support which would be considered a contribution directly or indirectly to political parties or candidates, including through intermediary organizations, such as political action committees or campaign funds. For example, IBM will not purchase tickets or pay fees for you or anyone else to attend any event where any portion of the funds will be used for election campaigns. In many countries, political contributions by corporations are illegal. IBM will not make such contributions, even in countries where they are legal. Also, the company will not provide any other form of support that may be considered a contribution.

You must not make any political contribution as a representative of IBM. You may not request reimbursement from IBM, nor will IBM reimburse you, for any personal contributions you make. In addition, you should recognize that your work time or use of IBM assets is the equivalent of such a contribution. Therefore, you will not be paid by IBM for any time spent running for public office, serving as an elected official or campaigning for a political candidate, unless required by law. You can, however, take reasonable time off without pay for such activities if your IBM duties permit the time off and it is approved by your manager. You also may use vacation time for political activity.
SCHEDULE "C"

Conflicts of Interest
V - Conflicts of Interest

A "conflict of interest" occurs when your private interest interferes in any way, or even appears to interfere, with the interests of the Company. A conflict situation can arise when you take actions or have interests that may make it difficult to perform Company work objectively and effectively. It is also a conflict if outside activities affect your judgement to act in the best interest of customers, investors and other stakeholders.

Conflicts of interest damage the trust between you, the public and the Company. To help prevent conflicts, you must complete a conflict of interest disclosure statement. You are responsible for updating the statement as your circumstances change.

If a potential conflict arises, report it immediately. If you need advice, consult the procedures described in the section of this Code titled "Where to go for help". The following are some of the most common areas of potential conflict, but the most reliable guideline is your own common sense.

DEAL AT ARM'S LENGTH WITH SUPPLIERS

You must not be associated in any way with agreements between the Company and suppliers or any organization in which you or a member of your immediate family have an interest or which might result in your or your family member's personal gain.

BRIBERY AND KICKBACKS ARE PROHIBITED

Manulife Financial does not allow unfair business practices such as rebating, bribery or kickbacks. These practices are against Company policy in all places where we do business.

BE CAREFUL ABOUT GIFTS

Offers of gifts and entertainment are courtesies common among business partners. However, offering or accepting gifts, entertainment or other benefits can be mistaken for improper payments. For this reason, you must not give or accept gifts, gratuities, favours or benefits if they are for more than a nominal value or if they go beyond what could reasonably be considered ethical and accepted business practices, or which may influence or appear to influence the performance of your duties.
BE CAREFUL ABOUT PERSONAL BENEFITS

Conflicts of interest may arise if you, or a member of your family, receives a personal benefit as a result of your position in the Company. All such personal benefits, including loans and guarantees of obligations from the Company, must be disclosed on the Company's Conflict of Interest Statement and approved by the Company. Personal loans to executive officers are prohibited unless specifically permitted by law.

FOLLOW COMPANY POLICY ABOUT HIRING FAMILY

In some situations, hiring or managing family members can lead to conflicts of interest, unethical employment practices and the appearance of special treatment. Family members must not be in positions that put them under or give them the direct or indirect supervisory authority of another family member. Family members include spouses (as defined for benefit purposes), children, siblings and parents. This applies to all employment, including full-time and part-time regular, contract and summer student hiring. All hiring within Manulife should be conducted by Divisional Staffing areas.

INVEST IN AN ETHICAL MANNER

Directors, officers and employees must strictly follow all laws and regulations affecting investment. It is unethical and illegal for directors, officers and employees to buy or sell Manulife Financial securities with the benefit of material information that has not been publicly disclosed about the Company or its affiliates or to inform another person, other than in the ordinary course of business, of material information that has not been publicly disclosed. In addition, it is unethical and illegal to buy or sell securities of other companies with the benefit of your knowledge of the Company's investment intentions or any information that has not been publicly disclosed about such other company and that you obtained in the course of your employment with Manulife Financial.

Directors, officers and employees must also be cautious of potentially being in a conflict of interest where they wish to make an investment in a business entity which they know transacts business with Manulife or in which Manulife has made an investment.
WORKING FOR COMPETITORS MAY JEOPARDIZE THE COMPANY

Unless a higher level senior executive has given prior written approval, no Manulife Financial director, officer or employee may work for any organization that competes with the Company or that has a business relationship with the Company. That includes serving as a director, officer, trustee, partner, employee, consultant or agent.

USE CAUTION REGARDING OUTSIDE POSITIONS

Outside work or financial involvement in external organizations can lead to conflicts of interest. Such involvement could interfere with your ability to give objective, full-time attention to your work with Manulife Financial or could damage the Company’s image. You must not engage in any other employment or take any civic, government or political position that would hamper your performance or your judgement to act in the Company’s best interest. You may sell merchandise on Company property only with the authorization of your manager or a Human Resources representative.

PROTECT CORPORATE OPPORTUNITIES

Directors, officers, employees, representatives and other associates are prohibited from (a) benefiting from opportunities that are discovered through the use of Company property, information or position; (b) using Company property, information or position for personal gain; and (c) competing with the Company. You owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises.

PROTECT THE COMPANY’S NAME AND ASSETS

The name Manulife Financial must be used only for authorized Company business and never for personal activities. Do not identify yourself with the Company while pursuing personal, political or not-for-profit activities, unless you obtain the Company’s authorization first.

Each director, officer, employee, representative or other associate entrusted with access to or control over Company transactions and assets must ensure that each use, acquisition or disposition of an asset by a person on behalf of the Company is undertaken with the general or specific authorization of management and is accurately and fairly recorded in reasonable detail in the Company’s books of account and record.
WHAT IS A CONFLICT OF INTEREST?
A "conflict of interest" occurs when your private interest interferes in any way, or even appears to interfere, with the interests of the Company as a whole. A conflict situation may arise when you take actions or have interests that may make it difficult to perform Company work objectively and effectively. It is also a conflict if outside activities affect your judgement to act in the best interest of customers or other stakeholders.

Please remember that:

➤ you must conduct your outside activities or interests on your own time, not during your hours of employment with Manulife Financial

➤ Manulife Financial resources, such as employees, equipment and supplies, may not be used for personal purposes

➤ outside activities and family or personal relationships must not interfere with your ability to exercise good judgement or perform your duties in a satisfactory way.

WHAT ACTIVITIES OR CIRCUMSTANCES SHOULD I REPORT?
Manulife’s Code of Business Conduct and Ethics will help you decide whether you are involved in activities or circumstances that you should report as a potential conflict of interest.

The types of activities you should report include:

➤ you or a family member receiving a personal benefit, including a loan or guarantee of obligation from the Company, as a result of your position in the Company

➤ having a job, trade or business outside Manulife Financial which could put you in direct or indirect competition with Manulife Financial, its suppliers, or others who have a contract with Manulife Financial

➤ becoming an officer, agent or director of a for-profit company

➤ reporting to or supervising a spouse, child, sibling, or parent, either directly or indirectly, at Manulife Financial or a subsidiary company

➤ having any family or other personal relationship with a Manulife Financial employee or service provider which could create the perception of a conflict of interest
any other situation that could reasonably appear to create a potential conflict of interest.

HOW SHOULD I REPORT A POTENTIAL CONFLICT OF INTEREST?
For officers, employees, representatives and other associates, where appropriate, you should also tell your manager about any real or possible conflicts of interest so that together you can address the issues involved. If you have discussed your situation with your manager, please indicate this on the disclosure statements (page 24) and include details.

WHAT DOES THE COMPANY DO WITH THESE STATEMENTS?
If you report a potential conflict, the Human Resources Department and/or Law Department will review your disclosure statement on a confidential basis. The process varies, depending upon the type of activity or relationship you report. The objectives of the review are to:

- assess whether you have any real or perceived conflict of interest, and
- take appropriate measures to address any conflict.

The Human Resources Department and/or Law Department may contact you for more details. You may also be asked to respond to any concerns raised by the review. Your manager may also take part in these discussions with you. Any understandings or agreements reached as a result of these discussions will be put in writing in an acknowledgement letter to you, together with a copy of your disclosure statement, and filed with the Human Resources Department.

WHAT SHOULD I DO IF MY SITUATION CHANGES?
It is your responsibility to keep the information you report up-to-date by filing a new disclosure statement. You can obtain the form from your divisional Human Resources Department or at @mfc in North America.

WHO SHOULD I CONTACT IF I HAVE QUESTIONS OR CONCERNS?
You may contact either Human Resources or the Law Department on a confidential basis if you have any questions or concerns about these guidelines or filing your report disclosure statement.
MEMBERS OF THE BOARD OF DIRECTORS

Members of the Board of Directors should address any real or possible conflicts of interest with the Company's General Counsel. Individual directors may also retain outside advisors, at the Company's expense, to provide advice on any matter before the Board or a Board Committee with the prior approval of the Corporate Governance & Nominating Committee.

It is the responsibility of every member of the Board of Directors to keep relevant information up to date by filing a new disclosure statement. The form should be filed with the Corporate Secretary.

A member of the Board of Directors may contact the Corporate Secretary on a confidential basis regarding questions or concerns about these guidelines or filing a disclosure statement.

See Code of Business Conduct and Ethics Acknowledgement and Conflict of Interest Disclosure STATEMENT HR2200EN
Code of Business Conduct and Ethics Acknowledgement and Conflict of Interest Disclosure Statement

COMPANY POLICIES AND GUIDELINES

I acknowledge that throughout the course of my employment/relationship with the Company, I agree to adhere/have and will continue to adhere to the Code of Business Conduct and Ethics and related corporate policies and guidelines of The Manulife Financial Corporation and its related companies ("Manulife Financial").

CONFLICT OF INTEREST

I have read and agree to follow the requirements for reporting potential conflicts of interest described in "Guidelines for Completing The Code of Business Conduct and Ethics Acknowledgement and Conflict of Interest Disclosure Statement" and in Manulife Financial's Code of Business Conduct and Ethics. I also agree to update the information I report on a continuous basis by completing a new disclosure form if my circumstances change.

Please check one of the boxes:

☐ I have no potential conflict of interest.

☐ I have a potential conflict of interest as described below. (Provide details, including the name of any outside employer, organization or business, the position you hold, a description of the family or personal relationship involved, etc.)
I have discussed this potential conflict with my manager or other appropriate personnel.

☐ No

☐ Yes (please provide date and a brief description)

<table>
<thead>
<tr>
<th>Date (mm/dd/yyyy)</th>
<th>Description</th>
</tr>
</thead>
</table>

Personal details and signature

Name [first, middle initial, last]
Employee Number
Title
Business Unit or Branch
Manager's Name
Date Signed [mm/dd/yyyy]
Signature

Send completed disclosure statement to your divisional Human Resources Department.
• AIG employees must not permit any business decision, such as a decision as to whether AIG will do business with an insured, producer, intermediary, reinsurer, prospect, counterparty or supplier to be influenced, or appear to be influenced, by interests unrelated to AIG. A decision to place AIG business with such entities and the volume of such business must be based solely upon business considerations.

• AIG employees owe a duty to AIG to advance AIG’s legitimate business interests when the opportunity to do so arises. AIG employees are prohibited from taking for themselves (or directing to a third party) a business opportunity that is discovered through the use of corporate property, information or position, unless AIG has been already offered and declined the opportunity.

• AIG employees must not knowingly permit themselves to be placed in a position where their interest could be perceived as potentially or actually adverse to AIG’s.

• Transactions involving AIG and a member of an AIG employee’s immediate family (e.g., spouse, child, sibling, parent or in-law) or an individual who has a close personal relationship with an AIG employee must be brought to the attention of the AIG employee’s manager to determine if the transaction poses a perceived, potential or actual conflict of interest.

• An AIG employee must maintain sound personal financial conditions so as to avoid any distractions that may prevent him or her from carrying out his or her responsibilities to AIG.

• An AIG employee must maintain the confidentiality of AIG’s business information both during and after his or her employment with AIG. This includes, but is not limited to, human resources and employee salary and benefits information, business strategies and plans and other proprietary information, as outlined in this Code and the relevant AIG policies and procedures relating to confidentiality, privacy and theft of trade secrets.

• An AIG employee planning to leave AIG may not solicit or encourage another AIG employee to leave the employment of AIG.
In all matters related to gifts or entertainment, it is the responsibility of the AIG employee to exercise good judgment. Offering and/or accepting gifts and entertainment is appropriate provided there is a specific business purpose, the expenses incurred are ordinary and necessary and the gift or entertainment falls within the guidelines of the AIG Travel and Entertainment Policy, this Code and all relevant laws and regulations. http://aignet.aig.com/corpadm/domplcy/T&E Expenses

- AIG employees may not accept or present a gift or entertainment (including, but not limited to, beverages, recreation, lodging, transportation and tickets) for the purpose of improperly influencing good business judgment in any business dealing or transactions involving AIG or any business or enterprise associated with AIG.

- A gift is any item of monetary value presented to an AIG employee by a non-AIG employee or any item of monetary value presented to a non-AIG employee by an AIG employee.

- Entertainment (including, but not limited to, beverages, recreation, lodging, transportation and tickets) is an event with a specific business purpose. Entertainment must include the presence of an AIG employee. AIG does not consider entertainment of a non-AIG employee as a gift, as long as both an AIG employee and a non-AIG employee are present during the event.

- Minimal value means retail value in the United States at the time of acceptance of $150.00 or less.

Gifts
Accepting Gifts

- An AIG employee may accept and retain gifts of minimal value, if the value of the gift is in line with accepted business practices and could not be construed as improperly influencing good business judgment. AIG employees may not receive gifts on a regular or frequent basis from the same source. The AIG employee is responsible for determining that a gift is of minimal value at the time of acceptance.
An AIG employee who has been offered a gift or entertainment that exceeds minimal value and therefore cannot be personally accepted under this Code, may accept the gift on behalf of AIG; if refused, reimbursement at the fair-market value or return would cause offense or embarrassment or would otherwise adversely affect the relationship of AIG to the gift giver. A tangible gift of more than minimal value is deemed to have been accepted on behalf of AIG and, upon acceptance, shall become the property of AIG.

If an AIG employee accepts a gift of more than minimal value, the employee must submit a written gift report to his or her manager within thirty days. Managers are responsible for collecting gift reports and filing them with the Internal Audit Department. Holiday season gift reports must be filed by February 1. AIG Domestic Corporate Policy Guide, Business Expense Policy- http://aignet.aig.com/corpadmin/dmplyc

Offering Gifts

Gifts must be in good taste and without excessive expense.

Prior written approval from a manager is required before purchasing a gift whose value equals or exceeds minimal value as established by this Code. Verbal approval by a manager is sufficient to order gifts whose costs are between U.S. $25 and $150, however, the expense must be approved in writing by a manager. AIG Domestic Corporate Policy Guide, Business Expense Policy- http://aignet.aig.com/corpadmin/dmplyc

Entertainment

Accepting Entertainment

Invitations for excessive or extravagant entertainment or invitations for entertainment not in good taste and/or without a specific business purpose must be declined.

If a non-AIG employee is not present at an entertainment event paid for by a non-AIG employee, the entertainment should be regarded as a gift and subject to the monetary gift limitation discussed above.
Offering Entertainment

- Entertainment offered by an AIG employee must be for a specific business purpose and in good taste.

- If an AIG employee is not present at an entertainment event paid for by the AIG employee, the entertainment will be deemed a gift and subject to the monetary gift limitation discussed above.

Outside Business Activities

For-Profit

- AIG employees must obtain written approval from their manager/department head before accepting outside employment or serving as a director, trustee, officer, owner, partner or consultant of a for-profit organization, regardless of whether compensation of any form is received. The AIG employee’s manager should send a copy of the written approval to the AIG Corporate Legal Compliance Group.

Not-For-Profit

- AIG employees desiring to serve as a director, trustee, officer, owner or partner of a not-for-profit organization as a volunteer and without compensation (for example, on the board of a school, hospital, cooperative or social organization) need not obtain prior approval if there is no actual, potential or perceived conflict of interest. If an actual, potential or perceived conflict of interest does arise, AIG employees must avoid even the appearance of impropriety in association with their conduct. All conflicts of interest should be disclosed to the AIG Corporate Legal Compliance Group.

Honorariums

- An AIG employee who is compensated for making an oral presentation, writing a magazine article or engaging in similar activities prepared or conducted using the time or facilities of AIG must report that compensation in writing to his or her manager. Such compensation, other than nominal honorariums ($150 or less) appropriate under the circumstances, will either be declined or paid to AIG.
5.0 ON YOUR OWN TIME

5.1 Conflicts of Interest

Your private life is very much your own. You are, however, an IBMer both on and off the job and a conflict of interest may arise if you engage in any activities or advance any personal interests, at the expense of IBM's interests. It's up to you to avoid situations in which your loyalty may become divided. Each individual's situation is different, and in evaluating your own, you will have to consider many factors. The most common types of conflicts are addressed here to help you make informed decisions.

5.1.1 Assisting a Competitor

An obvious conflict of interest is providing assistance to an organization that markets products and services in competition with IBM's current or potential products or service offerings. You may not, without IBM's consent, work for such an organization in any capacity, such as an employee, a consultant or as a member of its board of directors. Such activities are prohibited because they could divide your loyalty between IBM and that organization.

5.1.2 Competing against IBM

Today, many IBM employees are engaged on their own time in routine activities that involve technology, business insight, personal computers, software or other products that IBM offers to its clients. Generally, such activities do not result in a conflict of interest. However, employees should be careful to avoid activities that conflict with IBM's business interests.

Obviously, you may not commercially market products or services in competition with IBM's current or potential product offerings. Such marketing activities are "commercial" if you receive direct or indirect remuneration of any kind. Performing such activities on a noncommercial basis, such as through participation in a management approved Open Source project, is usually permissible, but not if IBM decides that the activities have or may have more than a minimal impact on IBM's current or future business.

Because IBM is rapidly expanding into new lines of business and new areas of interest, the company will constantly redraw lines of acceptable activity. It is unlikely that you will find definitive answers to many of your questions regarding the boundaries of acceptable activity in published guidelines. It is therefore your responsibility to consult with your management or IBM counsel to determine whether your planned activity will compete with any of IBM's actual or potential businesses. This should be done before you pursue any activity that might create a conflict of interest with IBM.

5.1.3 Supplying IBM

Unless approved in advance by senior management and IBM counsel, you may not be a supplier to IBM, represent a supplier to IBM, work for a supplier to IBM or be a member of its board of directors while you are an employee of IBM. In addition, you may not accept money or benefits of any kind for any advice or services you may provide to a supplier in connection with its business with IBM.
SCHEDULE “D”

Proper Use of Corporate Assets
competitor in any manner which would give us an undue competitive advantage

- employees who provide access services to competitors have a responsibility to ensure that this information is not made available to those within the Company or its affiliates who develop competitive service strategies

- we must not disclose a business partner's choice of competitive carrier to anyone who does not clearly require the information to provide service to the business partner.

- For other precautions in dealing with competitors, see Bell Canada's Canadian Competition Law Compliance Handbook, available by calling the Business Conduct Help Line at 310-6600, no area code required or send an email to ethics@bell.ca.

Reciprocity

Like many large corporations, we purchase goods and services from thousands of suppliers, many of whom are also our business partners. One of the most delicate questions in purchaser-supplier relationships is reciprocity — the promotion of sales through the use of purchasing power.

Reciprocity is an arrangement that both a purchaser and a supplier might be tempted to seek. For example, we, as a purchaser, might consider giving our business to a supplier who happens to be our business partner, in preference to another supplier who is a competitor's business partner. Similarly, a supplier may demand that it get our business because it is one of our major business partners.

While we quite naturally want to do business with our business partners, and will take advantage of every opportunity to do so, we must keep in mind that this should not be done at the expense of price, quality and service. These criteria, rather than the simple fact a supplier is or is not our business partner, should guide our purchasing decisions.

Reciprocity, whether it originates with the buyer or the seller, should be handled with utmost care for a number of financial, ethical and legal reasons. Under certain circumstances, we may, for strategic marketing reasons, develop and contract services exclusively with a given supplier. The Law Department must be consulted before all such arrangements are established.}

G. SAFEGUARDING COMPANY ASSETS

We all have a responsibility to safeguard Company assets. This is crucial to maintaining the trust and confidence of shareholders, as well as others who have a stake in the Company. The improper use and/or reporting of assets could seriously undermine the Company's integrity, adversely affect our business strategies and decisions and weaken investor confidence. It could also constitute a criminal offense.

Each of us is accountable for the protection of the Company's assets in our care, both physical (material, buildings, people, property, information, revenues) and logical (communications networks, information systems, intellectual property). Access to and use of these assets must be authorized, adequately controlled and based on business needs. Use for personal purposes of the Company's assets is strictly prohibited. Each of us must also take appropriate measures to prevent losses due to wilful action by others, both outside and within the Company, which may result in personal injury, property damage, theft,
CODE OF BUSINESS CONDUCT

loss, abuse or unauthorized access to physical or logical assets, and intellectual property (including data).

In the course of protecting Company assets, all employees are required to read, be aware of and comply with the BCE Security Charter and all Corporate Security policies which can be found on the Corporate Security web site (security.bell.ca).

It is our duty to promptly report to Corporate Security or the Business Conduct Help Line all acts that may constitute real or suspected breaches of security.

Further information may be found on the Corporate Security web site at security.bell.ca, in the following security policies:

BCE Security Charter

BCE IT Security Policy 3.1.1 Information Security

BCE IT Security Policy 5.1 Asset Accountability

BCE IT Security Policy 6.3 Security Incident Reporting

BCE IT Security Policy 7 Physical and Environmental Security

BCE IT Security Policy 9.1 Business Requirement for Access Control

Funds

We must properly use and protect Company cash, cheques, postage, etc., and ensure that all expense vouchers, benefit claims and invoices are accurate and properly authorized.

We must provide receipts and/or explanations for all expenses incurred on behalf of the Company.

We must charge all transactions to the appropriate accounts. We may only use corporate credit cards, charge cards, gasoline cards and calling cards for business purposes.

We should, whenever possible, use the services of business partners with whom the Company has negotiated agreements (for example, travel agents, car-rental agencies, taxi companies, hotels, etc.).

Books and Records

The Company's books and records contain vital information about all aspects of our operations. They form the basis upon which key decisions about the Company are made — whether internally, by Company executives and other management staff, or externally, by financial analysts, shareholders, investors, regulators, and so on.

Because they are so crucial to the proper running of our business, we must ensure that all documents, reports and records falling under our responsibility are accurate and complete. We must also ensure that all transactions are properly authorized.

In preparing and maintaining our books and records, we will:

• adhere to all accepted accounting standards and practices, rules, regulations and controls applicable to us

• ensure that all entries are recorded accurately and on time, in the proper accounts, and are properly documented

• record all funds, assets and transactions. We may not establish any undisclosed or unrecorded fund or assets for any purpose

• keep books and records which reflect fairly, accurately and in reasonable detail the Company's transactions, acquisition and disposal of assets and other relevant activities

• sign only those documents we believe to be accurate and truthful

• restrict access to sensitive or confidential information (such as financial records and business partner information) to ensure the information is not accidentally or intentionally disclosed, modified, misused or destroyed

• ensure, through an internal control process, that the Company meets its book- and record-keeping obligations.
Code of Business Conduct

Contract and Agreement Standards
Contracts and agreements represent some of the greatest exposures faced by the Company. They also represent a great opportunity for the Company to minimize retained risks. If you are in a position to develop or sign contracts, as per BCE's Schedule of Authorities, you must take necessary steps to protect the interests of the Company by ensuring that the contract is reviewed by appropriate departments such as, but not limited to, Legal, Regulatory and Risk Management. The Legal, Regulatory and Risk Management contacts are available to assist you, as well as to conduct individual contract reviews at your request.

IS/IT and Network Security
Computers and computer networks have become an essential feature of our workplace. Indeed, they form the very backbone of our telecommunications network and operations infrastructure. For this reason, every effort must be made to protect the Company's computer systems and associated software from the various threats to their security, such as accidental or deliberate destruction of data and equipment, interruption of service, disclosure of sensitive information, theft and corruption.

We must all comply with the following computer security policies:

- access to computer systems is granted only to authorized users
- users are responsible and accountable for their access to and use of computer systems; all access codes and passwords must be kept confidential
- the use of the Company’s computer system or network for personal use or other non-Company purposes is strictly prohibited, unless a manager in direct line of authority grants permission
- we must follow Company rules regarding the purchase and use of computer software
- to guard against computer viruses that may damage the Company's computer systems and jeopardize network security, we must check all new files regardless of source (e.g. e-mail attachments, internet, diskettes, etc.) with the latest version of a virus protection program
- each of us is responsible for reporting any breach of computer security, policies and standards.

For further information, see the following policies located on the Corporate Security web site at http://security.bell.ca:

- BCE IT Security Policy 3.1.1 Information Security
- BCE IT Security Policy 5.1 Asset Accountability
- BCE IT Security Policy 6.3 Security Incident Reporting
- BCE IT Security Policy 7 Physical and Environmental Security
- BCE IT Security Policy 8.3 Malicious Software
- BCE IT Security Policy 9.1 Business Requirement for Access Control
- BCE IT Security Policy 12.1 Legal Requirements

Personal Use of Company-Provided Internet Access

Access to the Internet is primarily provided for business purposes. However, accommodating employees' development and awareness needs through personal use of Company-provided Internet access is also encouraged. Personal use must be reasonable, i.e. it must not impede or reduce an employee's ability to perform his/her duties, diminish productivity or effectiveness at work or negatively impact the Company in any way. We are responsible for any of our action taken while using the Internet or e-mail and will be held accountable.

For the complete policy and important restrictions, see the "Bell Canada Internet Policy" located at address http://rhbell.canadahr.int.bell.ca and choose Your Workplace then access Internet Policy.
CODE OF BUSINESS CONDUCT

I'm attending an important meeting next week and I have to prepare a presentation using slides and fairly complicated charts. My friend has the software I need to put the presentation together, and he's offered to lend me his diskettes so I can install the program on my computer. Can I go ahead?

No. The law strictly prohibits the use of software on unlicensed computers. You must verify and respect the manufacturer's conditions of license or agreement under which the software was acquired. By copying your colleague's software into your computer, you may be breaking the software company's licensing agreement as well as copyright laws, and placing the Company at risk of prosecution for copyright infringement. You should speak to your group's computer administrator to discuss your computer needs.

Property

We must protect the physical and intellectual property of the Company and third parties from loss, damage, theft, vandalism, sabotage or unauthorized use, copying, disclosure or disposal. We must also ensure proper, business use only of Company and third party property; use of such property for personal purposes is strictly prohibited. This applies to property located in the office, at home or on business partner premises.

- physical property includes offices and office equipment, telephone equipment (both wireline and cellular/wireless), tools, vehicles, etc.

- intellectual property refers to such things as patents, copyrights, moral rights, trademarks, domain names, integrated circuit topographies, industrial designs, trade secrets, confidential information, know-how, business methods and processes, computer software, computer operating systems, written materials (including in paper or electronic form), inventions, graphics, photographs, audio-visual documents, etc. (see next page for more on inventions).

Upon termination of employment or contract, or reassignment, we must return all physical and intellectual property of the Company or entrusted to the Company in our possession.

For further information on loss, theft, damage of Company property, refer to BCE IT Security Policy 7 Physical and Environmental Security

For further information on how to submit an opportunity to sell BCE's Intellectual Property to another party, refer to http://ip-group.intranet.bell.ca.

What should I do if I discover that a Company trademark has been infringed or misused?

Trademarks, along with the Company logo and Company trade names, are among our most valuable assets, and every employee has a responsibility to preserve, protect and enhance these assets. You should immediately report any infringement or misuse of a Company trademark or trade name, as well as the Company logo, to the Branding and Identity line at (514) 870-2347

For further information on trademarks, see the Brand Intranet site at address: http://brand.intranet.bell.ca, or contact the Branding and Identity line at 514-870-2347

Intellectual Property

Intellectual Property is amongst the most valuable assets of the Company. Protecting our innovation and our brands enhances our competitive edge and solidifies our freedom to operate.

All intellectual property such as inventions, works and other intellectual property assets described in the previous section conceived or made during or after working hours in the course of our employment with the Company, or which is within the scope of the Company's business interests, are rightly the property of the Company.

We are prohibited from disclosing the Company's proprietary information and intellectual property such as trade secrets, inventions, marketing plans, etc. outside the Company without ensuring
that the proper safeguards and legal documentation are in place. Failure to do so could make the Company lose its right in a trade secret or its right to file a patent for an invention.

We are prohibited from attempting to apply for a patent or other type of protection of intellectual property, such as a trademark, domain name, industrial design or copyright registration, in relation to an invention, work or other intellectual property that we conceived or made during or after working hours in the course of our employment with the Company, or which is within the scope of the Company's business interests, or to make use of it for personal gain.

We must fully disclose to our manager and to the Intellectual Property Group all intellectual property that we conceived or made during or after working hours in the course of our employment, or which is within the scope of the Company's business interests, and such works are hereby automatically assigned to the Company, without limitation as to territory, duration or otherwise, all rights, including intellectual property rights, in and to all such intellectual property, without charge, in order to enable the Company to, among others, apply for patents in the Company's name in any country.

All moral rights that we may have under the Copyright Act (Canada) (or any successor or similar legislation in other jurisdictions or at common law) in, or related to, the intellectual property that we conceived or made during or after working hours in the course of our employment with the Company, or which is within the scope of the Company's business interests are irrevocably waived in favour of the Company and its affiliates.

You must cooperate fully in the preparation and execution of all necessary documents if the Company decides to use/sell the intellectual property or to apply for protection, registration or enforcement of intellectual property rights.

You may apply to be released from the obligation to assign specific intellectual property rights to the Company. Each case will be examined on its own merit and the Company will be reasonable in this regard.

For further information on BCE's management of Intellectual Property, refer to "Intellectual Property Policy and Guidelines" or to apply for Intellectual Property Awards please refer to the web site http://ip-group.intranet.bell.ca.

Visible ID
Every employee, consultant and contractor must wear a valid, designated ID card at all times while on Company premises. Visitors must wear a valid, designated visitor's card while on Company premises and employees should challenge anyone on Company premises not wearing one.

H. A WORK ENVIRONMENT BASED ON TRUST AND RESPECT

Nothing is more basic to ethical behaviour than trust and respect. A work environment that encourages and values trust and respect also makes good business sense: it enables us to build and cultivate more meaningful, richer relationships with fellow employees, business partners and shareholders.

The Company is committed to fostering such a workplace, one which:

✔ recognizes the intrinsic dignity and worth of all employees
✔ values, encourages and leverages the diversity of all employees, business partners and shareholders
✔ enables all employees to work without fear of intimidation, discrimination, harassment or violence
✔ encourages open and honest communication
✔ makes reasonable effort to accommodate the particular needs of all employees
✔ enables all employees to work safely.

Diversity in the Workplace

Diversity is defined as an unwavering respect for each other's uniqueness. Culture, ethnicity, gender, age, religion, disability, sexual orientation, education and experiences are just some of the facets of diversity. By valuing our differences, we can create an inclusive work environment based on merit and fairness where all employees can contribute to their fullest
Protecting Corporate Property

We have an obligation to safeguard corporate assets by ensuring they are properly maintained and used to further GM business interests. We should always consider whether our decision to use or commit a GM resource is in the best business interest of the Corporation. In this regard, Corporate assets should not be used for personal purposes. However, there are often situations where infrequent and limited personal use of GM assets is permissible (for example, a local phone call home). When such situations arise, discuss the issue with your leader if you are not sure if the use is appropriate.

Internet/E-mail and Voice Mail Usage

As a general rule, use of the Internet, like other GM assets, should be limited to situations related to our work assignments. Nominal personal use is permitted so long as it is reasonable, ethical, does not interfere with work responsibilities and/or productivity, and is not in conflict with GM’s Acceptable Use Policy found at http://ilm.gm.com/policies_05.html or directions from your local leadership. If in doubt, you should ask our leadership.

It is never acceptable to use GM E-mail or the Internet to access, transmit or store pornographic material or sexually oriented jokes or cartoons.

It is never acceptable to use GM equipment or information systems (such as E-mail and the Internet or intranet) to access or create material that is illegal or in poor taste, or when it interferes with our work responsibilities or when it is in conflict with local management directives. In that regard, all employees must refrain from any illegal, unethical, unauthorized, or disruptive use of GM information systems and equipment. This would include, but is not limited to, accessing, transmitting or storage of inappropriate material (e.g., pornography, lewd or violent materials, chain letters, sexually oriented jokes or cartoons, and/or other offensive/demeaning material related to age, race, color, sex, religion, national origin, disability or sexual orientation). Violations of GM’s policy in this regard will subject you to possible disciplinary action up to and including discharge.

If you receive an inappropriate message from a fellow employee or source external to GM, tell the sender to stop and delete the message so it cannot be transmitted to another party. If such messages persist, report the matter to your leader for corrective action.
Confidential and Proprietary Information

The loss or misuse of GM information can undermine our competitive position in the marketplace. Each of us has a responsibility to safeguard any proprietary and confidential information entrusted to us.

Confidential information includes, but is not limited to, future product plans or proposals, pricing, technical specifications, financial data, marketing and sales programs and product costs. General guidelines for protecting confidential information include:

- Refraining from discussing sensitive GM business in public, including in restaurants and on airplanes;
- Using password protection on computers and computer files and not posting or otherwise disclosing these passwords to others; and
- Securing and locking files, desks and cabinets.

Our responsibility to protect GM information extends even after we leave General Motors employment. We must return all GM records (including documents and files, electronically readable or otherwise), and continue to safeguard any GM information that we possess.

Communicating With the Media

Providing clear and accurate communication to the media and general public maintains integrity in our relationships with the public. Because of its importance, all GM business units have a designated public affairs or communications function that is responsible for communicating GM’s position on a range of issues.

If you are contacted by a member of the press, the best course of action is to first discuss the situation with your leader and your business unit’s communication representative to ensure that the most appropriate person or team responds. Employees are under no obligation to immediately respond to a journalist. Responsible members of the media do not expect impromptu answers. As a general rule, even if you are the subject matter expert, you should not respond to media questions without first consulting with a GM communications representative and following their advice. With respect to pending lawsuits or investigations, there should be no public statements without prior approval of Legal Staff.
DO


- Treat all GM information, and other types of GM property as business assets belonging to someone else — GM's stockholders.

- Be alert to your surroundings — do not discuss sensitive GM business in public places.

- Take steps to ensure that our communications are accurate — whether internal or external.

- Maintain all GM records in accordance with GM Information LifeCycle Management Policies.

- Comply with all applicable laws and regulations, and GM's Acceptable Use Practices governing the use of GM information resources, such as computers, software, E-mail, the Internet and intranet (Socrates) and telecommunications devices.

DON'T

- Bypass or circumvent security procedures to save time.

- Provide access to GM information to anyone not authorized to have it.

- Use GM property or systems for our own personal profit or gain, or for political activity.

- Create or knowingly process misleading or inaccurate information about our company business.

- Use GM information resources to create, access, transmit, or store any material that would be considered in bad taste, offensive, disrespectful of others, or otherwise inappropriate.

- Engage in any activity that would disrupt or compromise the availability, integrity or security of GM information, information resources or other types of GM property.
Integrity of Our Information and Property

Use of GM Property

All GM employees have an obligation to protect the Corporation's assets and ensure their efficient use. GM's assets include not only cash and other financial assets but also plant and equipment, inventory, supplies, information and information technology. GM assets should be used only for GM business purposes. For example, GM's fleet of company-owned vehicles serves the exclusive purpose of furthering GM's interests. If we operate a company-owned vehicle, we are required to adhere to the highest standards of safety, including observance of all terms of the GM Safe Driving Program. We must observe proper authorization procedures for any assignment or use of a company-owned vehicle.

Unauthorized use of office telephones for personal calls and similar seemingly innocuous "minor" personal uses of GM property also can be wrong. If we abuse or take unfair advantage of our access to GM property and use it for personal needs that result in more than nominal cost to GM, we have betrayed GM's trust in us, misappropriated GM's assets, and sacrificed our integrity.

Submitting false expense reports is a clear example of misappropriating GM assets, as is copying GM-supplied software for personal use. Using GM-supplied laptops or personal computers for personal projects carries additional data security and risks contamination (e.g., by viruses) of GM's applications and data.

Information Security

Information is one of our most valuable assets in the competitive global marketplace for our products and services. We all share a responsibility to protect and manage valuable GM information, records and other property for our mutual benefit.

The GM Information Security Policy and Practices (ISP&P) [http://iss.gm.com/tech/gsd/infosecurity/gm_ispp/index.html] are the authoritative source for detailed guidance on the classification and protection of GM information. The GM Information LifeCycle Management (ILM) Policies [http://ilm.gm.com/] are the authoritative source for detailed guidance on the creation, maintenance and disposal of all GM records containing GM information, and for the Acceptable Use Practices (AUP) that govern our use of GM information resources, such as our computers, e-mail systems, the Internet and GM intranet (Socrates), and telecommunications equipment such as our telephones and fax machines. Both of the foregoing policies apply to the third parties, including contract workers who handle or have access to GM information.
These policies reflect our recognition that General Motors information is one of GM's most important assets. The high value we place on our information derives from its impact on our business. We could lose a competitive advantage if competitors learn about our future product information. We could lose customers if competitors beat us to the market with our own innovations. We could lose our operational effectiveness if GM business records are not available to meet the business needs of the company, including the legal, tax and other regulatory requirements where GM conducts its business.

Each of us must learn and comply with the GM Information Security and LifeCycle Management requirements and Acceptable Use Practices applicable to our job duties and activities. This includes everything from securing our workstations and refraining from discussing sensitive information on crowded elevators or with those not having a need to know, such as competitors, suppliers, consultants, friends or even family, to keeping passwords secret and following the GM record retention schedule and disposal guidelines in the ISP&P and ILM Policies. In addition, we need to recognize and take steps to guard against monitoring or interception risks associated with using cellular phones, fax machines, electronic mail, etc. When traveling, especially internationally, we must always be alert to the possibility of various forms of eavesdropping on airplanes or in airports, restaurants and even hotel rooms. We must also recognize the potential harm from computer viruses, worms and other forms of malicious code, and avoid risky behavior that could create the possibility of malicious code being introduced into GM computing systems.

GM information includes all information related to our business, created or acquired using GM resources, regardless of the specific nature, medium or form of the information.

All GM information is considered proprietary, that is, the property of GM, and must be protected by GM employees against unauthorized disclosure, modification, or destruction. GM information, including information about GM's activities, business plans, products and employees, must not be disclosed outside GM without leadership approval from the GM unit responsible for the GM information.

Some GM information is competitively sensitive and could create adverse consequences if disclosed. This GM information is "classified" for additional protections in two broad categories: (1) information resulting from GM investment of resources that is unique and has competitive value to GM, — and (2) information that, if disclosed, could have adverse consequences for GM, including, for example, financial loss, negative effects on GM's Corporate image or breaches of some legal duty or agreement. Within these broad categories, information may be classified as "GM SECRET," or "GM CONFIDENTIAL." The principal differences between the "GM SECRET" and "GM CONFIDENTIAL" classifications are the value of the GM information, the potential degree of damage from unauthorized disclosure and the number of individuals to whom the information has been disclosed.
### In the Workplace

#### "GM SECRET"
- Is the most restrictive.
- Requires the most protection.
- Known by a limited number of individuals.
- Often considered strategic or trade secret.
- Likely to cause irreparable damage to the competitive position of a business unit, or to GM as a whole, if disclosed.

#### "GM CONFIDENTIAL"
- Is less restrictive.
- Also requires controls.
- Distributed only to those with a "need to know."
- Likely to cause substantial competitive or financial damage to GM if disclosed.

#### Examples:
- Payroll information.
- Personnel information.
- Plant rationalization plans.
- Technical data.
- Software written for GM applications.
- Legal documents marked to indicate confidentiality.
- New engineering specifications.
- Computer passwords.

---

We all must recognize the value of GM information and our individual and collective responsibility for its protection. Our information can be found everywhere—from computers and computer networks to desk drawers; from voice mail to business planners and briefcases; and from file drawers to conference room walls and even the plant floor.

Before the public release of GM information (e.g., at conferences, in technical publications, etc.), obtain proper authorization. This will ensure that the release will serve GM's business needs. Of course, an official GM announcement or public speech relieves us of the obligation to maintain the security of the released information. In fact, when GM publishes information, we may be encouraged to assist in its dissemination.

While we are obligated to protect and properly manage information, we all need to be mindful that GM property of all types, both material and intellectual, is not ours. Modifying, using, removing or disposing of GM information or any other GM property without authorization is theft, and can be treated as such.
Examples

Information Security

Example

Bill works in the Marketing Department of one of the vehicle divisions and is responsible for the incentives recommendations on several passenger cars. He is at a cocktail party in his neighborhood and one of his friends casually asks whether GM will be putting any incentive money on one of its more popular models. Bill doesn't specifically tell his friend exactly what the incentive will be, but winks and suggests that his friend not purchase the vehicle in the next 30 days. Joe, an Auto Executive for another car company, is standing nearby and hears Bill's comments without meaning to eavesdrop. Joe is new to the neighborhood and Bill had not yet met him.

Jane is a Vehicle Engineer working on a future engine design. To save some time on a recent trip, she pulled out some reading material, including several confidential memos concerning the development strategy and possible applications of her project while she was seated on the plane. She thought she was being discreet, but the person next to her was able to see the basic contents of the memos. He never spoke to Jane, but he was a Design Engineer with similar responsibility for a major competitor. The timetable and extent of the future product development was far more extensive than any public report had revealed. He reported back to his leadership what he had seen on the flight.

Analysis

The message of both these examples is that we all share a responsibility to safeguard appropriately the proprietary and confidential information we see in our day-to-day assignments. Moreover, failure to be alert to our surroundings can compromise important GM plans and strategies. Discussions and document reviews in public places like airports, elevators and even neighborhood parties can do great damage to GM. We must all take information security very seriously at all times.
Example

Daryl is a Tech Specialist at the Technical Center. While searching the Internet for product-related technical information, he finds a Web site called "Autotech Tools" containing what appear to be several copyrighted programs containing executable code that he downloaded to his personal computer. He then sent copies of the executable programs to four of his coworkers. The next day he opens the first program he downloaded and finds that it contains a new computer virus that his computer's antivirus software doesn't yet recognize and cannot eradicate. Before he can warn his coworkers, he and they become infected with the virus resulting in the unrecoverable scrambling of 23 departmental directories that contained testing analysis for four auto-adjusting suspension systems.

Analysis

Daryl should have realized that the Internet can pose a serious information security risk to GM and its computing resources. All computer system users must adhere to GM's Acceptable Use Practices in the ISP&P and ILM Policies when using the Internet. Among the ILM Acceptable Use Practices is the directive that: "Users must not load or install unauthorized or illegal software on GM-provided computing equipment, including, but not limited to, personally owned images or software, freeware, shareware, games, screen savers, graphics, Web browser 'plug-ins,' or software that may expose the company to copyright infringement claims."

He also should have paid attention to the copyright designations of the programs he was downloading as their use could have serious legal ramifications to GM. It is every employee's duty to abide by all applicable laws and regulations, including laws and regulations pertaining to copyrights, trademarks, and patents, and protection of data, trade secrets and software.
Example

Susan is a Web Administrator for an internal GM Web site. She received a request from Bob, a GM financial planner, to post several documents on the Web site she manages. The documents included a Five-Year Business Plan, a forecast of increased market distributions, future program dates, proposed cost figures and a return on investment analysis. Sue posted the documents as requested.

John, the manager of the group, was browsing the GM intranet and was upset after finding this data. He knew that the majority of the information was “GM Confidential” and should have only been shared on a “need-to-know” basis. He had no idea that the information would be posted out on the internal GM Web and hadn’t given his approval. He noticed the documents were not labeled and no precautions had been taken to protect the information. He called Susan and asked for the material to be removed immediately until appropriate steps could be taken.

Analysis

This situation highlights several problems. The information had not been appropriately classified as described in the GM Information Security Policy and Practices. The “GM Confidential” information was not properly posted, and John’s group had no approval process for posting information on their Web site. A lot of competitive harm could result if that GM information fell into the wrong hands, even inadvertently.

Many GM Web sites have both a public area, available to all employees, and a private area, restricted to authorized GM employees. GM Confidential Information should be ID and password protected, and GM Secret information should not be posted without strong authentication, authorization and encryption mechanisms.
SCHEDULE "E"

Protection of Confidential Information
Confidential information
As an employee, officer, or member of the board of directors, you should take every precaution to keep Nortel Networks and third-party confidential information in confidence. These guidelines will assist you, but if you have further questions or concerns, contact your manager, Business Ethics, or the Law Department.

What is confidential information, and what are my responsibilities for protecting it?
There are two principal categories of Nortel Networks confidential information and both are key corporate assets. The first is our non-public technical information such as product plans, future product direction, technical information concerning Nortel Networks products and services, manufacturing and development process information, engineering designs, drawings and layouts, software code, trade secrets, know-how, pending patent applications, invention disclosure statements and the like. The second is non-public business information such as non-public financial information, employee information (including e-mail lists), analyses, forecasts, customer lists, strategic and operating plans, corporate organization plans, audit materials or reports, legal opinions and advice, information regarding litigation or potential litigation, proposed transactions, and the like.

The release (intentional or inadvertent) of any of our confidential information to third parties without appropriate controls and/or protections can damage Nortel Networks and in some cases violate the law. For example, inappropriate release of confidential technical information can diminish Nortel Networks rights to this information, may give others implied rights to it that we would not have knowingly permitted, or may cause us to lose valuable information to competitors. It could provide our competitors with the solution to an important problem, or allow them to avoid costly research and development. If competitors gain even a general sense of what we intend to bring to market, they may get a head start in countering our competitive advantage.

Also, unauthorized release of our non-public business or financial information can have serious legal implications under certain circumstances. Securities laws mandate that "material" non-public information not be selectively disclosed to some (such as investment analysts, individual investors, the media, or any other members of the public) but not others. Our Disclosure Committee strictly regulates disclosure of non-public material information. If your work requires you to discuss such information with outsiders (in negotiating a transaction, for example), such discussions should occur only with the protection of a non-disclosure agreement. Generally, information will be considered material if:

- There is a substantial likelihood that a reasonable investor would consider it important in making an investment in Nortel Networks securities, or would view the information as having significantly altered the "total mix" of information available about Nortel Networks;
- Public disclosure of such information would reasonably be expected to have a significant impact on the market price or value of Nortel Networks securities.

Some simple guidelines for protecting Nortel Networks confidential information:

1. If you are discussing company business in restaurants, on airplanes, in elevators, or on mobile phones in public places, be very sure you can't be overheard. Think twice before transmitting confidential materials via mobile phones, fax, and e-mail, and use encryption technology where feasible when transmitting confidential information over the Internet or mobile phones. For information about encryption software, see the Information Services website at http://pki.ca.nortel.com/
2. If you see Nortel Networks confidential information left unattended or otherwise made accessible to people who should not have it (even other Nortel Networks employees), report this immediately to your manager. Discuss confidential information only with those employees who have a legitimate need to know.

3. Make sure that tangible or electronic copies of any Nortel Networks confidential information are clearly marked "NORTEL NETWORKS CONFIDENTIAL" or "NORTEL NETWORKS CONFIDENTIAL – SPECIAL HANDLING" depending on the appropriate classification of the material and according to Corporate Procedure 205.04 on the Protection of Confidential Information.

4. Disclose confidential information to a third party only where there is a compelling business reason to do so. Even then, disclose such information only when protected by a signed and delivered non-disclosure agreement, or a license agreement that sets out the obligation of the third party to keep our information confidential and limits their use of the information to the purposes specified in the agreement or license.

5. When engaging in discussions or negotiations that involve disclosing Nortel Networks confidential information to third parties under a non-disclosure agreement, make sure that no statement, agreement, or transfer of technology is made that inadvertently grants the party a license or rights to use Nortel Networks intellectual property (e.g. patents, industrial designs, copyrights in software, documentation or graphics, trade secrets, mask works/integrated circuit topographies, or trademarks).

6. Ensure that an intellectual property review of any strategic, technical, or design information has been done to preserve Nortel Networks patent or other intellectual property rights. In particular, once a new product or technical concept has received preliminary approval or development, you should promptly consult with the IP Law group to begin this review, to make sure patentable inventions are identified and appropriate intellectual property protection addressed. The disclosure or publication of an invention or sale of a product without proper patent application protection may, for example, cause Nortel Networks to forfeit its potential patent rights to the invention.

Confidential information of third parties:

Just as we have obligations to protect our own confidential information, we have obligations with respect to the confidential information of third parties. Improper handling of sensitive business, financial, or technical information, or of original ideas provided to us by customers, suppliers, and other third parties with whom we have a business relationship, can lead to a loss of trust and/or liability for damages. Another significant risk that arises from handling information of such third parties, including Nortel Networks competitors, is that our own development activities in the area relating to the improperly obtained or used confidential information may be foreclosed or inhibited. For example, we may be independently working on an idea, technology, or product similar to that described in the confidential information, and could have our efforts stalled, or subject to significant penalties, by claims of misappropriation made against Nortel Networks by the owner of that confidential information.

You may be provided with third-party confidential information in furtherance of a legitimate business purpose. Such information may come to you under the terms of a confidentiality agreement that limits the use that Nortel Networks may make of such information and places restrictions on the handling or distribution of such information. Be sure that you carefully track and manage the third-party information, and ensure that Nortel Networks strictly abides by the terms of any such agreement.
PROTECTING INFORMATION

OVERVIEW
It is your obligation to safeguard the company’s nonpublic information. You should not share this information with anyone outside the company unless it is necessary as part of your work responsibilities.

Nonpublic information is any information that has not been disclosed or made available to the general public. Trading in stocks or securities based on nonpublic information, or providing nonpublic information to others so that they may trade, is illegal and may result in prosecution.

Nonpublic information includes items such as financial or technical data, plans for acquisitions or divestitures, new products, inventions or marketing campaigns, personal information about employees, major contracts, expansion plans, financing transactions, major management changes and other corporate developments.

GENERAL PRINCIPLES
• Do not disclose nonpublic information to anyone outside the company, except when disclosure is required for business purposes and appropriate steps have been taken to prevent misuse of the information.
• Employees may not buy or sell stocks or securities based on nonpublic information obtained from their work at the company.
• Disclosing nonpublic information to others, including family and friends, is a violation of the Code and may violate the law.
• Just as the company values and protects its own nonpublic information, we respect the nonpublic information of other companies. If you have any questions about obtaining or using nonpublic information of other companies, contact company legal counsel for guidance.
• Records should be retained or discarded in accordance with the company’s record retention policies. Consult with company legal counsel regarding retention of records in the case of actual or threatened litigation or governmental investigation.
THE CODE IN REAL LIFE

The action: A marketing manager was preparing a presentation on a new company promotion. She was excited about the plan and wanted to discuss it with a friend outside the company. She wasn't sure if that would be a Code violation, so she checked with her manager.

The decision: It's a good thing she checked. Sharing nonpublic information is a Code violation, even if the recipient doesn't work for a competitor, customer or supplier.

The action: An administrative assistant heard an office rumor that the company was considering acquiring a small, publicly traded beverage firm. She wondered if it was OK to acquire some of the stock of the other beverage company. She asked her manager.

The decision: Don't buy the stock, the manager said, after seeking advice from company legal counsel. It's a violation of the Code and a violation of securities laws on insider trading. She didn't buy the stock—it wasn't worth going to jail or losing her job.

The action: A manager was seeking a supplier to provide construction work for the company and received three sealed bids for the job. The manager gave his favorite firm the details of the competing bids so that firm could win the business.

The decision: That was wrong. The manager disclosed nonpublic company information and circumvented the bidding process. He was disciplined.

The action: A company attorney was traveling with a colleague on a plane to work on a legal case. They began to discuss the particulars of the case when one of them noticed a man across the aisle listening intently and taking notes.

The decision: They quickly decided it was time to drop the subject. It's never a good idea to discuss company matters in public where others might hear and take advantage of the information.

The action: After an important competitor held a meeting at a hotel, a hotel security guard offered a tape recording of the meeting to a company employee. The company employee wasn't sure what to do, so he took the tape to his manager.

The decision: The company employee should never have taken possession of the tape. It was wrong. No one listened to the tape, and the employee's manager promptly returned it. But even so, the competitor learned of the situation and brought a claim against the company.
SCHEDULE “F”

Fair Dealing with Others
analogue mode) do not provide a secure method of communication

- returning all proprietary information and documents provided by the Company, including all third party information entrusted to the Company, upon termination of employment or contract, or reassignment.

Any attempt to obtain proprietary information by unauthorized means or to misuse such information should be reported to a manager immediately.

Further information may be found in the booklet “Security is Everyone’s Business or on the Corporate Security website (http://security.bell.ca), in the following policies:

- BCE IT Security Policy 5.2 Information Classification
- BCE IT Security Policy 8.7.7 Voice, Fax and Video Security

How do I tell if a document (paper or electronic) is proprietary if it is not marked as such?

You should begin by asking the person who issued the document if known, as the originator is the person who must determine the classification. If you can’t find the source of the information and the nature of the document does not make the classification obvious (such as information that has been made public), the document should be treated as Restricted until the proper classification is determined.

Use of Confidential Information

Many of us have access to confidential information which is not available to the general public, or which has not yet been made public. Using this information for purposes other than furthering the Company’s best interests is not only unethical, it may be illegal if it involves the disclosure of material non-public information. Using any confidential or privileged non-public information about the Company for personal purposes, or failing to safeguard such information, is strictly prohibited.

F. DEALING WITH BUSINESS PARTNERS AND COMPETITORS

To achieve a sustained and enduring competitive advantage, we must ensure that our reputation for quality, service and integrity remains unimpeachable. The best way to maintain our reputation – and strengthen our competitive advantage – is to compete fairly and vigorously while complying fully with our legal and ethical obligations. Fair competition means that we respect our business partners, competitors, agents and all alliance partners.

Relations with Business Partners

Our Company service often involves a visit to a business partner’s home or place of business. Over the years, we have acquired an enviable reputation for honesty, courtesy, integrity and respect for property in dealings with business partners. With vigorous competition in the communications marketplace, this reputation has become more valuable than ever.

Selling our Products and Services

Our business partners trust us to provide quality products and services, and be truthful when discussing our advantages and benefits. To maintain that trust:

- we offer business partners only those services which we are legally allowed to provide, either alone or through contract with an alliance partner or agent, at approved rates and charges, where applicable
- we sell only those products and services our business partners want and need
- we promote our products and services accurately
- we give business partners the straight facts about their competitive choices
- we guide business partners into asking the right questions about their competitive options
- we don’t offer to waive charges, cut special deals or grant discounts that are not authorized; we don’t do anything that suggests we are “buying business”.

© BCE Inc/Bell Canada 2004 - All Rights Reserved
Depending on the products and services involved, this kind of behaviour could violate CRTC regulations and/or provisions of the competition law, as a result, the Company and possibly the employee might be subject to legal action.

**Treating Competitors with Respect**

We welcome and encourage competition and we are committed to treating competitors with due respect. By doing so, we honour the competitive spirit that motivates us to perform at our best.

We have a responsibility to portray our competitors fairly, accurately and without bias. Acting otherwise will result in charges of anti-competitive behaviour, and possibly in lawsuits.

Behaving competitively means that:

- we do not portray a competitor to the public or to a business partner in an inaccurate, misleading, disparaging or unfair manner
- we do not state as a fact our understanding of a competitor’s price information as that information may be out of date and incomplete
  - we are careful about commenting publicly, or to a business partner, on such topics as a competitor’s financial situation, business practices, management or network reliability, or foreign ownership. It is often hard to pin down the correct facts about these matters, and we can be accused of misrepresentation. The best source of information about a competitor comes from the competitor itself. If facts about a competitor are public knowledge, direct the business partner to the source of this information (i.e., newspaper report, magazine article, TV or radio news item).
- we do not behave spitefully or disrespectfully toward a business partner who has decided to purchase a competitor’s products or services; we continue to rigorously promote and provide high-quality service for any other product we may supply to this business partner.

**Obtaining information about our Competitors**

We have every right to gather information about the marketplace in which we operate. This includes information about our competitors, their products and services, technology, prices, advertising, and so on. However, we must only obtain this information through legal and ethical channels. Acting otherwise is against the law and may result in prosecution.

- we do not engage in industrial espionage
- we do not buy proprietary competitive intelligence (such as marketing plans, sales strategies, etc.)
- we must never induce another employee to obtain confidential information, nor must we request or induce the employee of a competitor to provide such information.

- Our business unit recently hired someone who held an executive position with one of our competitors. This person was deeply involved in planning the competitor’s expansion strategy, and he has information which would be very valuable to us. Can we ask him to disclose this information?

- Absolutely not. The new employee has an obligation to protect his former company’s confidential or proprietary information, just as you would be obliged to protect BCE’s confidential or proprietary information if you were to leave the Company. You must respect the employee’s personal integrity as well as his obligation to his former employer.

**When a Competitor is a Business Partner**

In our competitive environment, competitors are also our business partners. When serving business partners who are also competitors, we must keep the following points in mind:

- we must never use information obtained as a result of providing service to the
CODE OF BUSINESS CONDUCT

competitor in any manner which would give us an undue competitive advantage

- employees who provide access services to competitors have a responsibility to ensure that this information is not made available to those within the Company or its affiliates who develop competitive service strategies

- we must not disclose a business partner's choice of competitive carrier to anyone who does not clearly require the information to provide service to the business partner.

- For other precautions in dealing with competitors, see Bell Canada's Canadian Competition Law Compliance Handbook, available by calling the Business Conduct Help Line at 310-6600, no area code required or send an email to ethics@bell.ca.

Reciprocity

Like many large corporations, we purchase goods and services from thousands of suppliers, many of whom are also our business partners. One of the most delicate questions in purchaser-supplier relationships is reciprocity – the promotion of sales through the use of purchasing power.

Reciprocity is an arrangement that both a purchaser and a supplier might be tempted to seek. For example, we, as a purchaser, might consider giving our business to a supplier who happens to be our business partner, in preference to another supplier who is a competitor's business partner. Similarly, a supplier may demand that it get our business because it is one of our major business partners.

While we quite naturally want to do business with our business partners, and will take advantage of every opportunity to do so, we must keep in mind that this should not be done at the expense of price, quality and service. These criteria, rather than the simple fact a supplier is or is not our business partner, should guide our purchasing decisions.

Reciprocity, whether it originates with the buyer or the seller, should be handled with utmost care for a number of financial, ethical and legal reasons. Under certain circumstances, we may, for strategic marketing reasons, develop and contract services exclusively with a given supplier. The Law Department must be consulted before all such arrangements are established.

- Our department is organizing a meeting at a hotel. Due to the large size of our group, and the fact we don't want to travel far, we've chosen a nearby hotel serviced by a competitor's long distance network. Is this okay, or should we find a hotel that uses Bell Canada long distance?

- It is not our policy to prohibit employees on Company business from dealing with organizations that do not use Bell Canada's services. While we actively encourage everyone to do business with our business partners, we must ensure that this is not done at the expense of price, quality and service.

- Although the hotel you've chosen is not a Bell Canada business partner, you were right to choose it if, in your judgment, it best meets the price-quality-service criteria you are looking for: the hotel is located close to your office, it can easily accommodate all the members of your department and, as a result, will enable your group to save both time and traveling expenses.

G. SAFEGUARDING COMPANY ASSETS

We all have a responsibility to safeguard Company assets. This is crucial to maintaining the trust and confidence of shareholders, as well as others who have a stake in the Company. The improper use and/or reporting of assets could seriously undermine the Company's integrity, adversely affect our business strategies and decisions and weaken investor confidence. It could also constitute a criminal offense.

Each of us is accountable for the protection of the Company's assets in our care; both physical (material, buildings, people, property, information, revenues) and logical (communications networks, information systems, intellectual property). Access to and use of these assets must be authorized, adequately controlled and based on business needs. Use for personal purposes of the Company's assets is strictly prohibited. Each of us must also take appropriate measures to prevent losses due to wilful action by others, both outside and within the Company, which may result in personal injury, property damage, theft,
that the proper safeguards and legal documentation are in place. Failure to do so could make the Company lose its right in a trade secret or its right to file a patent for an invention.

We are prohibited from attempting to apply for a patent or other type of protection of intellectual property, such as a trademark, domain name, industrial design or copyright registration, in relation to an invention, work or other intellectual property that we conceived or made during or after working hours in the course of our employment with the Company, or which is within the scope of the Company’s business interests, or to make use of it for personal gain.

We must fully disclose to our manager and to the Intellectual Property Group all intellectual property that we conceived or made during or after working hours in the course of our employment, or which is within the scope of the Company's business interests, and such works are hereby automatically assigned to the Company, without limitation as to territory, duration or otherwise, all rights, including intellectual property rights, in and to all such intellectual property, without charge, in order to enable the Company to, among others, apply for patents in the Company’s name in any country.

All moral rights that we may have under the Copyright Act (Canada) (or any successor or similar legislation in other jurisdictions or at common law) in, or related to, the intellectual property that we conceived or made during or after working hours in the course of our employment with the Company, or which is within the scope of the Company’s business interests are irrevocably waived in favour of the Company and its affiliates.

You must cooperate fully in the preparation and execution of all necessary documents if the Company decides to use/sell the intellectual property or to apply for protection, registration or enforcement of intellectual property rights.

You may apply to be released from the obligation to assign specific intellectual property rights to the Company. Each case will be examined on its own merit and the Company will be reasonable in this regard.

**Visible ID**

Every employee, consultant and contractor must wear a valid, designated ID card at all times while on Company premises. Visitors must wear a valid, designated visitor's card while on Company premises and employees should challenge anyone on Company premises not wearing one.

**H. A WORK ENVIRONMENT BASED ON TRUST AND RESPECT**

Nothing is more basic to ethical behaviour than trust and respect. A work environment that encourages and values trust and respect also makes good business sense: it enables us to build and cultivate more meaningful, richer relationships with fellow employees, business partners and shareholders.

The Company is committed to fostering such a workplace, one which:

- Recognizes the intrinsic dignity and worth of all employees
- Values, encourages and leverages the diversity of all employees, business partners and shareholders
- Enables all employees to work without fear of intimidation, discrimination, harassment or violence
- Encourages open and honest communication
- Makes reasonable effort to accommodate the particular needs of all employees
- Enables all employees to work safely.

**Diversity in the Workplace**

Diversity is defined as an unwavering respect for each other’s uniqueness. Culture, ethnicity, gender, age, religion, disability, sexual orientation, education and experiences are just some of the facets of diversity. By valuing our differences, we can create an inclusive work environment based on merit and fairness where all employees can contribute to their fullest
Fair Competition and Antitrust

Compete and deal fairly with our customers, suppliers and competitors and use caution to avoid violating antitrust and competition laws.

We believe in fair and open competition, and our success depends in part on our ability to offer competitively priced quality products and services. While we compete vigorously, we comply with applicable antitrust and competition laws wherever we do business.

Antitrust or competition law is extremely complex and covers a broad range of conduct that may be declared illegal. Many antitrust or competition laws prohibit making agreements with competitors or customers to limit or restrict competition, or sharing information with competitors or customers that would limit or restrict competition. This information could include discussions or agreements with competitors relating to:

• prices,
• products and services,
• business practices,
• territories,
• bids for new business,
• distribution channels, or
• customer lists.

As a general rule, you should avoid discussing these topics with competitors. If a competitor raises any of these topics, you should interrupt and stop the conversation immediately. If you attend a conference and have informal contact with a competitor, it is always a good idea to limit informal contact to the extent possible and keep a written summary of any discussions that may have taken place. The standards for conspiracy to violate antitrust laws are extremely broad and an unlawful agreement can be found where competitors never met or exchanged words, but did something like share competitive information. Antitrust violations do not have to be proven by written agreements and violations can be inferred from an individual’s or organization’s actions. It’s a good idea to use extreme care when talking with competitors or potential competitors.

Because antitrust or competition law is so complex and varies significantly from country to country, you should consult the Thomson legal department in advance of any planned actions that might be considered anti-competitive.

We also deal fairly with our customers, suppliers and competitors. While comparative marketing and advertising are generally acceptable, employees should not unfairly disparage or criticize competitors’ products or services. While we strive to exceed customers’ expectations, we will only make honest and factual claims about our products, services and businesses that can be substantiated. Employees should also not seek to obtain information about our competitors through unlawful or unethical practices.

Q: I’m planning to attend an industry conference and anticipate that I will meet my “equivalent” at a principal competitor. I’ve heard through the grapevine that we are both planning to bid on a new service contract for Corporation XYZ. Can I speak to him?

A: Maybe. You should speak to the Thomson legal department first before you initiate any conversations with a competitor that may pertain to things like pricing and costs. Even an informal discussion at a conference can be a potential antitrust or competition law violation.
Equal Employment Opportunities

We provide a workplace that offers equal employment opportunities (EEO).

We are committed to providing equal employment opportunities (EEO) for all persons regardless of:

- race,
- color,
- religion,
- gender,
- age,
- marital status,
- sexual orientation,
- national origin,
- citizenship status,
- disability,
- veteran status, or
- any other group protected by applicable federal, state or local laws.

This policy extends to all terms and conditions of employment, including, but not limited to, hiring, placement, promotion, termination, layoff, recall, transfers, leaves of absence, compensation and training. We comply with applicable laws governing nondiscrimination in every location in which we have facilities.

Thomson makes every effort to reasonably accommodate individuals with a disability in order to provide employment opportunities for them. Furthermore, it is the company's commitment not to discriminate in any manner against qualified individuals with disabilities with regard to all terms and conditions of employment. Employees who believe they have a disability that may require a reasonable accommodation in order to perform the essential functions of their position should contact their manager or the Human Resources department.

Q: I am planning to promote one of two employees. One is a man, and the other is a woman who has been talking in the office from time to time about her plans to eventually start a family. Can I promote the man if I think the woman is likely to have children soon and might leave the company?

A: No, this would be a violation of our policy. In the United States, for example, a promotion based on these facts would also violate applicable EEO laws.

Q: What is "reasonable accommodation" and what is a "disability"?

A: "Reasonable accommodation" may include, but is not limited to, altering facilities, providing a qualified reader and providing information orally. Additionally, in purchasing equipment or making changes to our facilities, Thomson strives to ensure that the adaptability and accessibility of equipment and facilities for disabled individuals are key considerations. However, in some instances, a particular accommodation may not be possible if it would impose an undue hardship on Thomson. Employee requests for reasonable accommodation should be brought to the attention of the Human Resources department immediately.

"Disability" refers to a physical or mental impairment that substantially limits one or more of an individual's major life activities. A disabled individual is an individual who has such impairment, has a record of such impairment or is regarded as having such impairment.

A qualified person with a disability is an individual who, with or without reasonable accommodation, can perform the essential functions of the position the individual holds or is applying for.
Equal Employment Opportunities

We provide a workplace that offers equal employment opportunities (EEO).

We are committed to providing equal employment opportunities (EEO) for all persons regardless of:

- race,
- color,
- religion,
- gender,
- age,
- marital status,
- sexual orientation,
- national origin,
- citizenship status,
- disability,
- veteran status, or
- any other group protected by applicable federal, state or local laws.

This policy extends to all terms and conditions of employment, including, but not limited to, hiring, placement, promotion, termination, layoff, recall, transfers, leaves of absence, compensation and training. We comply with applicable laws governing nondiscrimination in every location in which we have facilities.

Thomson makes every effort to reasonably accommodate individuals with a disability in order to provide employment opportunities for them. Furthermore, it is the company's commitment not to discriminate in any manner against qualified individuals with disabilities with regard to all terms and conditions of employment. Employees who believe they have a disability that may require a reasonable accommodation in order to perform the essential functions of their position should contact their manager or the Human Resources department.

Q: I am planning to promote one of my employees. One is a man, and the other is a woman who has been talking in the office from time to time about her plans to eventually start a family. Can I promote the man or the woman if I think the woman is likely to have children soon and might leave the company?

A: No, this would be a violation of our policy. In the United States, for example, a promotion based on these facts would also violate applicable EEO laws.

Q: What is "reasonable accommodation" and what is a "disability"?

A: "Reasonable accommodation" may include, but is not limited to, altering facilities, providing a qualified reader and providing information orally. Additionally, in purchasing equipment or making changes to our facilities, Thomson strives to ensure that the adaptability and accessibility of equipment and facilities for disabled individuals are key considerations. However, in some instances, a particular accommodation may not be possible if it would impose an undue hardship on Thomson. Employee requests for reasonable accommodation should be brought to the attention of the Human Resources department immediately.

"Disability" refers to a physical or mental impairment that substantially limits one or more of an individual's major life activities. A disabled individual is an individual who has such impairment, has a record of such impairment or is regarded as having such impairment. A qualified person with a disability is an individual who, with or without reasonable accommodation, can perform the essential functions of the position the individual holds or is applying for.
Discrimination and Harassment

Workplace discrimination and harassment will not be tolerated.

Employees need to know that they work in a safe and respectful environment where high value is put on equity, fairness and dignity. Thomson has zero tolerance for harassment. Harassment generally means offensive verbal or physical conduct that singles out a person to the detriment or objection of that person. Harassment covers a wide range of conduct, from direct requests of a sexual nature to insults, offensive jokes or slurs, and results in a hostile work environment.

No employee or non-employee may harass another employee, customer, vendor, supplier, visitor or any other person on company premises or while doing company business regardless of location. Harassment on the basis of race, color, religion, national origin, gender, age, disability, sexual orientation, marital status, citizenship status, veteran status and any other group protected by law and sexual harassment is prohibited by the company. In addition, conduct that does not violate the law but that is inappropriate is also prohibited.

Reports of harassment will be promptly and thoroughly investigated in as confidential a manner as possible. We will take immediate and appropriate action if harassment is determined to have occurred. Reprisals or retribution against an employee wholodges a complaint will not be tolerated. Reports of harassment should be made to your manager, your Human Resources department, or through the Thomson hotline (1.800.381.8266).

Q: I usually meet one of our suppliers every few months to discuss our upcoming requirements. One salesperson in particular regularly jokes around a lot and often tells me how sexy he thinks that I look. I don’t find this welcome. Can I do anything about this?

A: This may be a form of sexual harassment, which includes unwelcome sexual advances. Sexual harassment can come from customers and suppliers as well as fellow employees. This sort of conduct can create a hostile or intimidating environment. If you feel comfortable doing so, you should tell the salesperson that you find his conduct to be offensive. If you do not feel comfortable doing this, or if he fails to listen to you, you should report his conduct to your manager or your Human Resources department or use the Thomson hotline.

Q: Does this policy on discrimination and harassment apply outside of Canada and the United States? In the country in which I work, we have different standards.

A: Yes. All Thomson employees throughout the world should have a work environment in which they are shown respect by their colleagues.