Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy

Ver 4.5
Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy

Risks and Costs Associated with Email, Social Networking, Electronic Communication, and Mobile Devices

ENTERPRISE is faces many risks and cost as it comes to depend more on the new technologies. This policy must be followed in order to minimize to security risks and economic loss to ENTERPRISE. As new risks are identified these procedures will be updated. Some of the risks and costs that these procedures address are:

- The loss of general ENTERPRISE data and files.
- The disclosure to competitors of key financial data, sales contacts, suppliers, and strategies.
- The physical loss of a mobile device.
- The time to recover from the loss.
- The introduction of viruses and malware into the enterprise’s computer base, when synchronizing mobile device in the office and on a home PC.

Appropriate use of Equipment

The ENTERPRISE provides PC’s, PDA’s, laptops, servers, smartphones, USB Storage Devices, telephones, video players, televisions, and other equipment as tools for use by employees working on business objectives. This equipment is not to be used for personal use. Inappropriate use of the equipment, including installing non-business related software could result in appropriate disciplinary action up to and including termination. The systems are not to be used for commercial ventures, religious or political causes, outside organizations, or other personal matters unrelated to your job.

BYOD Security

By adopting strategies that are flexible and scalable and taking advantage of new and upcoming security features, ENTERPRISE will be better-equipped to deal with incoming challenges to their security infrastructure posed by the use of employees’ own devices.

- Follow the formal BYOD policies of ENTERPRISE
- Implement locking of the device after 5 minutes of inactivity
- Implement a remote wipe of the BYOD if the device is lost or stolen
- Limit the storage of sensitive and confidential information
Regulations and Industry Impact Table

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Industry Impacted</th>
<th>Retention Implications</th>
<th>Penalties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley</td>
<td>All publicly-traded companies</td>
<td>Audit records must be maintained for 7 years AFTER the audit</td>
<td>Fines up to $5,000,000 &amp; imprisonment up to 20 years</td>
</tr>
<tr>
<td>Section 17a-4</td>
<td>Financial Services</td>
<td>Email records must be kept for 3 years, trading records thru the end of the account plus 6 years</td>
<td>Case by case</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Healthcare</td>
<td>Hospital records must be kept for 5 years, medical records for the life of the patient plus 2 years</td>
<td>Fines up to $250,000 &amp; imprisonment up to 10 years</td>
</tr>
</tbody>
</table>

Keys to Email Archiving Compliance

In the e-discovery and compliance areas, establishing an audit trail is critical, allowing the company to demonstrate unequivocally that e-mails and other evidence have not been tampered with. Since many e-mails contain critical corporate or customer data that should not be accessible to just anyone, the capability may be useful from the standpoint of ensuring that critical data is not accessed by unauthorized users.

There are four objectives that must be met. They are:

- **Discovery** - Information must be easy to access and consistently available in to meet legal discovery challenges from regulatory committees.

- **Legibility** - Information must have the ability to be read today and in the future, regardless of technology. When selecting archiving technology, companies should look for solutions that are based on open systems, in the event that their Email application should change. For example, if a company migrates from Microsoft Exchange to Lotus Notes, they must still be able to quickly access and read archived Emails.

- **Auditability** - An Email archiving solution must have the ability to allow third parties to review information and validate that it is authentic.

- **Authenticity** - Information must meet all security requirements, account for alteration, and provide an audit trail from origin to disposition. An audit trail can track any changes made to an Email.
Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy

Internet & Electronic Communication - Employee Acknowledgment Form

If you have questions or concerns about this Policy, contact the ENTERPRISE’s CIO before signing this agreement.

I have read the ENTERPRISE’s electronic communication and Internet Usage Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including my termination.

Employee Name __________________________ ID Number __________________________

Job Title __________________________ Location __________________________

Do you need internet or computer training?

☐ No ☐ Yes (Intermediate)
☐ Yes (Novice) ☐ Yes (Advanced)

Signature __________________________

Approval Process

Supervisor □ Approved

IT Department □ Approved

User ID __________________________ Security Level □ Basic user

Comments

☐ Supervisor

Manager

System Administrator

1 Please retain one copy of this policy with your signature with your records and forward a copy of the signed page to the office of the CIO.
Internet Use Approval Form

It is the policy of ENTERPRISE that Internet use on behalf of the ENTERPRISE should be strictly limited to appropriate business purposes.

1. Access to Internet Services
   A. Employees must be authorized in writing by their management to use the ENTERPRISE’ resources to access and use Internet services. When necessary and appropriate, customers and suppliers or other third parties may be authorized, but only in writing, to use the ENTERPRISE’s resources to access and use Internet services.
   B. Access to Internet services may only be authorized after individuals agree in writing to abide by this policy.
   C. Management who authorizes the use of Internet facilities is responsible for promptly notifying the appropriate Internet administrator when the employee or authorized third party terminates, changes departments or no longer requires the use of Internet service so that access can be terminated.

2. Appropriate Uses of the Internet
   The Internet should be used for ENTERPRISE business, the performance of work-related duties and professional training and education. Electronic communications in furtherance of the ENTERPRISE’ business, activities with professional associates, colleagues, supplier representatives, and others is permitted.

3. Improper Uses of the Internet
   Although the Internet represents a valuable information resource for legitimate business and technical research and information sharing, it also presents a significant opportunity for abuse, lost productivity and potential liability for both the ENTERPRISE and the employee. The following are examples of activities, which could result in revocation of Internet access privileges or other disciplinary action, not excluding termination.
   A. Personal activities that incur additional costs to the ENTERPRISE or interfere with employee’s work performance.
   B. Profit-making activities that accrue to the employee.
   C. Political activities.
   D. Unlawful activities, including sending or receiving copyrighted materials in violation of copyright laws or license agreements.
   E. Sending or retrieving sexually explicit or offensive messages, cartoons or jokes, ethnic slurs, racial epithets or any other statement or image that might be construed as harassment, disparagement or libel.
   F. Sending ENTERPRISE proprietary or confidential materials to anyone not entitled to know or possess them.
What’s News

Version 4.5
- Updated to meet the latest mandated and regulatory compliance requirements
- Added Social Networking Policy Compliance Form
- Added Telecommuting Work Agreement Form
- Added Text Messaging Sensitive Information Form

Version 4.4
- Added a section on the Federal Rules of Civil Procedures
- Added a section on BYOD Security
- Updated compliance materials for auditing and e-discovery
- Listed 10 action steps to be followed in the enterprise’s acceptable use policy

Version 4.3
- Updated all of the forms
- Added section on Best Practices for Internet browsing

Version 4.2
- Updated Forms
- Added electronic version of forms
- Added reference section Canada's Anti-spam Law (CASL), Bill C-28
- Update styles

Version 4.1
- Added section on policies for tablets, PDA’s, and SmartPhones

Version 4.0
- Added Section for commercial Email
- Added Best Practices for Opt-In Email
- Reviews and revised policy to comply with all current security and privacy legislations

Version 3.3
- Added Social Networking Policy
- Update prior materials to include social networking policy
Version 3.2

- Updated Email retention and destruction with materials from the Records Retention and Destruction policy
- Expanded Email policy to include specifics on materials that are mandated to be archived

Version 3.1

- Updated policy to include email user best practices
- Updated style sheet to be CSS and WORD 2007 compliant
- Updated forms

Version 3.0

- Updated policy to cover mobile devices
- Added materials for Smartphones and USB Storage Devices
- Defined risks and costs associated with mobile devices
- Forms Added:
  - Internet & Electronic Communication – Employee Acknowledgement Form
  - Email Employee Acknowledgement Form
  - Internet Use Approval Form
  - Internet Access Request Form
  - Security Access Application Form

Version 2.2

- Added table for Regulations and Industry Impact

Version 2.1

- Email Forwarding Added