



## Written Information Security Program

### Agenda

---

- Background
- MGL 201 CMR 17.00 Requirements
- Written Information Security Program (WISP)
  - ✓Intention
  - ✓Program Description
  - ✓Policies
- Task List

### Background

---

#### Information Security Professionals

- ✓Identify security exposures
- ✓Find ways to eliminate them
  - Procedurally
  - Through technology

### MGL 201 CMR 17.00

---

- ✓Purpose is to protect an individual within the Commonwealth of Massachusetts from identity theft
- ✓Defines the standards to satisfy MGL c. 93H
- ✓Does not address all the security exposures an organization faces

## MGL 201 CMR 17.00 Requirements

---

Protection of "Personal Information" about a resident of the Commonwealth - information that legally identifies an individual.

- ✓ A person's first name and last name or first initial and last name in combination with
  - Social Security Number
  - Driver's license number or state-issued identification card number
  - Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password

Publicly available information does not apply.

## MGL 201 CMR 17.00 Requirements

---

Develop, implement, and maintain a written comprehensive information security program (WISP)

- ✓ Administrative, technical, and physical safeguards appropriate to
  - Size, scope, and type of business
  - Amount of resources available, "technically feasible"
  - Amount of stored data
  - Need for security and confidentiality of consumer and employee information

Risk-based approach

## MGL 201 CMR 17.00 Requirements

---

WISP must minimally

- ✓ Designate information security personnel
- ✓ Identify and assess foreseeable risks to the security, confidentiality and/or integrity of electronic, paper, or other records
- ✓ Establish safeguards or improve existing ones
  - Ongoing employee training
  - Employee compliance
  - Means for detecting security program failures
- ✓ Impose disciplinary measures for violations

## MGL 201 CMR 17.00 Requirements

---

WISP must minimally

- ✓ Develop policies for storage, access, and transportation of Personal Information outside of business premises
- ✓ Establish physical access restrictions including locked facilities and storage
- ✓ Prevent terminated employees from access

## MGL 201 CMR 17.00 Requirements

---

### WISP must minimally

- ✓ Oversee third party service providers
  - Select and retain only those capable of maintaining appropriate security measures
  - Require such documentation in a contract
  - New contract not required until March 1, 2012 for third parties with existing contracts before March 1, 2010



## MGL 201 CMR 17.00 Requirements

---

### WISP must minimally

- ✓ Specify regular monitoring to ensure that the WISP is effective
- ✓ Require annual review or review when change in business practice affects information security
  - WISP can and should evolve to reflect changing business environment
- ✓ Require documentation of responsive actions to breach of security



## MGL 201 CMR 17.00 Requirements

---

### Computer System Security Requirements

- ✓ Secure user authentication protocols
  - Control of user identifiers
  - Secure method of assigning and changing passwords
  - Secure storage of passwords
  - Restricting access to active users
  - Blocking access after multiple unsuccessful attempts to gain access



## MGL 201 CMR 17.00 Requirements

---

### Computer System Security Requirements

- ✓ Secure access control measures
  - Restrict access to records on "need to know" basis
  - Allows unique and traceable user identification and passwords to each individual
- ✓ Monitoring for unauthorized use or access
- ✓ Encryption of transmitted information
- ✓ Encryption on laptops and portable devices



### MGL 201 CMR 17.00 Requirements

#### Computer System Security Requirements

- ✓ Up-to-date system security agent software and malware protection
- ✓ Up-to-date operating system security patches and firewall protection for information accessed from the Internet
- ✓ Education and training of employees on proper use of security systems and the importance of personal information security



## **Written Information Security Program**



### Written Information Security Program

Intention

Program Description

Policies



### Written Information Security Program

Comprehensive in scope

- ❖ = Required by MGL
- ✓ = Generally recommended security practice
- [info in brackets] = areas that should be customized for each organization



## WISP - Intention

---

- ❖ Comply with MGL requirements for identity protection
- ✓ Protect organization from illegal or damaging actions
- ✓ Protect from disclosure of sensitive or confidential information
- ✓ Protect computer and electronic assets
- ❖ Document policy



## WISP - Description

---

- 1.0 Purpose
- 2.0 Roles and Responsibilities
- 3.0 Scope
- 4.0 Additional Terms and Definitions
- 5.0 Risk Assessment
- 6.0 Training
- 7.0 Monitoring, Enforcement and Violations
- 8.0 Revision History



## WISP - Description

---

### 1.0 Purpose

- ❖ Identify Personal Information
- ✓ Identify Confidential Information
- ❖ Define appropriate use of that information
- ❖ Incorporate policies and procedures for secure physical and electronic
  - storage
  - access
  - transportation within and outside of organization premises
- ✓ Define acceptable use of Computer Resources and Information Systems



## WISP - Description

---

### 2.0 Roles and Responsibilities

#### 2.1 Information Security Officer

- ❖ The *[insert job title]* will act as Information Security Officer:
  - Maintaining the WISP
  - Performing a review at least annually
  - Implementing, monitoring, and assessing associated policies
  - Overseeing the enforcement of policies and procedures



## WISP - Description

---

### 2.0 Roles and Responsibilities

#### 2.2 Personnel

- ❖ Every employee, temporary employee, intern, volunteer, and other contract worker
- ❖ Access to Personal and Confidential Information on a "need-to-know" basis
- ✓ Acknowledge understanding in writing
- ❖ Receive training in effective information security practices
- ❖ Upon termination, access blocked immediately



## WISP - Description

---

### 2.0 Roles and Responsibilities

#### 2.3 Third Parties

- ❖ Every contractor, consultant, and vendor who must have access to Personal or Confidential Information or to Computer Resources and Information Systems, e.g.,
  - Accountants, bookkeepers, payroll services
  - IT consultants, web developers, application support
  - Landlord, cleaning services
- ❖ Access to Personal and Confidential Information on a "need-to-know" basis
- ❖ Contract required specifying that Third Party will maintain appropriate security measures



## WISP - Description

---

### 3.0 Scope

- ❖ 3.1 Personal Information
- ✓ 3.2 Confidential Information
- ✓ 3.3 Computer Resources and Information Systems



## WISP - Description

---

### 4.0 Additional Terms and Definitions

- ✓ Used within the WISP and related policies
- ✓ Add additional terms if necessary

"Person, a natural person, corporation, association, partnership, or other legal entity [other than an agency . . . of the Commonwealth."



## WISP - Description

---

### 5.0 Risk Assessment

- ❖ Identify paper, electronic and other records, computing systems, and storage media, including mobile computing and storage devices that contain Personal and Confidential Information
- ❖ Identify where physical and electronic records containing Personal and Confidential Information are stored
- ❖ Identify which job positions and Third Parties require access to this information
- ❖ Identify when those records may be transported outside of business premises either via physical relocation or through electronic means



## WISP - Description

---

### 5.0 Risk Assessment

- ❖ On at least an annual basis
- ✓ Document in a confidential Annual Risk Assessment Report
- ❖ Revise policies and procedures where necessary



## WISP - Description

---

### 6.0 Training

Employees are the first line of defense in protecting the organization

- ❖ Required for all Personnel
- ❖ Proper use of computer security
- ❖ Importance of the security and privacy of Personal and Confidential Information
- ❖ Must be ongoing to reflect policy changes



## WISP - Description

---

### 7.0 Monitoring, Enforcement and Violations

#### 7.1 *Monitoring and Enforcement*

- ❖ Responsibility of the Information Security Officer

#### 7.2 *Violations*

- ❖ Personnel subject to disciplinary action, up to and including termination of employment.
- ❖ Third Parties subject to termination of any contracts or agreements.



## WISP - Description

---

### 7.0 Monitoring, Enforcement and Violations

#### 7.3 Breach of Security

- ❖ If the breach involved Personal Information, inform the appropriate state and federal agencies where necessary according to law.
- ❖ Inform any customers/ clients/ donors/ members whose Personal Information might have been compromised by the breach.



## WISP - Description

---

### 7.0 Monitoring, Enforcement and Violations

#### 7.3 Breach of Security

- ❖ Perform a post-incident review of the steps leading up to the breach
- ❖ Specify actions to be taken to avoid a similar incident in the future
- ❖ Revise policies and procedures
- ✓ Disseminate revisions to all Personnel and Third Parties as quickly as possible



## WISP - Description

---

### 8.0 Revision History

A summary of revisions:

*"February 28, 2010. Initial Written Information Security Plan and associated policies approved by ORG management and the Board of Trustees."*



## WISP - Policies



## WISP - Policies

---

- A: Access to Physical Records Policy
- B: Access to Electronic Records Policy
- C: Acceptable Use of Computer Resources and Information Systems Policy
- D: Password Control Policy
- E: Remote Access Policy
- F: Wireless Communication Policy
- G: Mobile Computing and Storage Device Use Policy
- H: Information Retention and Destruction Policy
- I: Email and Messaging Retention and Destruction Policy
- J: Website Security and Privacy Policy
- x: Access to Premises Policy (not included)



## A: Access to Physical Records Policy

---

### When do you need this Policy?

- ❖ If you store or handle Personal or Confidential Information recorded in physical form
  - ❖ Credit Card numbers
  - ❖ Checks
  - ❖ Social security numbers or EINs
  - Donor information
  - Etc.



## A: Access to Physical Records Policy

---

### 1.0 Purpose

- ❖ Protect Personal or Confidential Information recorded in physical form
- ❖ Define procedures for secure storage, access, and transportation of information

### 2.0 Policy

- ✓ Cannot be enforced through automated means
- ❖ Requires particular vigilance and awareness by Personnel and Third Parties



## A: Access to Physical Records Policy

---

### 2.1 Storage

- ❖ Personal or Confidential Information stored in locked facilities
  - Minimally a locked cabinet in a locked room
- ✓ Specify the locations used for Personal and Confidential Storage

### 2.2 Access to Premises

- ❖ Provide procedures regarding authorization and access to premises which might include:
  - Key assignment
  - Alarm system assignment and use



## A: Access to Physical Records Policy

---

### 2.3 Access to Information

- ❖ Personnel and Third Parties access Personal or Confidential Information on a "need to know" basis
- ✓ Personal or Confidential Information incorrectly received should be redirected to the proper department



## A: Access to Physical Records Policy

---

### 2.4 Transportation (❖ policy required)

- ✓ Personnel and Third Parties should keep Personal or Confidential Information out of plain sight
- ✓ Return documents to the secure location as soon as possible

### 2.5 Retention and Destruction

- ✓ Physical Records will be retained in accordance with Appendix H: Information Retention and Destruction Policy and Appendix I: Email and Messaging Retention and Destruction Policy.



## B: Access to Electronic Records Policy

---

### When do you need this Policy?

- ❖ If you store or receive Personal or Confidential Information recorded in electronic form
  - ❖ Credit Card numbers
  - ❖ Checks
  - ❖ Social security numbers or EINs
    - Donor information
    - Etc.



## B: Access to Electronic Records Policy

---

### 1.0 Purpose

- ❖ Protect Personal or Confidential Information recorded in electronic form
- ❖ Define procedures for secure storage, access and transportation

### 2.0 Policy

- ❖ All Personnel and Third Parties will be assigned unique user accounts and passwords
- ✓ Awareness of situations not covered



## B: Access to Electronic Records Policy

---

### 2.1 Secure Electronic Authentication Protocols

- ✓ Password reset by user on initial login
- ❖ Passwords not viewable by security personnel
- ❖ Access to network only by active, valid user accounts
- ❖ User access blocked after a set number of invalid attempts to login
- ✓ Computers automatically lock when idle for designated interval



## B: Access to Electronic Records Policy

---

### 2.1 Secure Electronic Authentication Protocols

- ✓ Personnel should log off unattended computers
- ❖ Security Officer to monitor unauthorized access attempts
- ❖ Firewall protection on systems
- ❖ Define procedure to detect security system failures
- ❖ Maintain up-to-date operating system maintenance, security software, malware protection



## B: Access to Electronic Records Policy

---

### 2.2 Storage

- ❖ Personal and Confidential Information will be protected from unauthorized access by security agent software
  - Files placed logically according to Information Retention and Destruction Policy
  - File and folder access controls will enforce "need to know" restrictions



## B: Access to Electronic Records Policy

---

### 2.3 Access

- ❖ Personal and Confidential Information access provided on a "need to know" basis
- ✓ Personnel and Third Party access based on job descriptions and contracts

#### *Unintended Access*

- ✓ Personal or Confidential information received by unauthorized Personnel or Third Parties will be delivered immediately to the authorized department



## **B: Access to Electronic Records Policy**

---

### *2.4 Transportation or Electronic Transmissions*

- ❖ Personal and Confidential Information will be encrypted when
  - Transmitted across public networks
  - Transmitted wirelessly
  - Stored on mobile computing and storage devices
  - On backup tapes and removable backup devices

### *2.5 Retention and Destruction*

- ✓ Electronic Records will be retained in accordance with Appendix H: Information Retention and Destruction Policy and Appendix I: Email and Messaging Retention and Destruction Policy.

## **C: Acceptable Use of Computer Resources and Information Systems Policy**

---

### When do you need this Policy?

- ✓ If you wish to clearly communicate to Personnel that computer resources are the property of the organization and are only to be used for business purposes

## **C: Acceptable Use of Computer Resources and Information Systems Policy**

---

### 1.0 Purpose

- ✓ Document Personnel and Third Party acceptable use of hardware, software, networks, storage media, websites and portable devices

## **C: Acceptable Use of Computer Resources and Information Systems Policy**

---

### 2.0 General Use and Ownership

- ✓ Data is property of the organization
- ✓ Personnel should limit private use
- ✓ Personnel must comply with Personal and Confidential data requirements
- ✓ Usage is subject to monitoring
- ✓ Usage is subject to auditing

### C: Acceptable Use of Computer Resources and Information Systems Policy

#### 3.0 Security of Personal and Confidential Information

- ✓ Personnel and Third Parties are responsible for passwords and accounts
- ✓ Disclaimer on Public Forums
- ✓ Know where sent email is going
  - List and group contents
  - Is information personal or confidential?



### C: Acceptable Use of Computer Resources and Information Systems Policy

#### 3.0 Security of Personal and Confidential Information

- ✓ Know where texting and messaging is going
  - Are recipients in a secure location?
- ✓ Do not automatically forward email outside network
- ✓ Use caution when opening attachments
  - Delete email with attachments from unknown sources



### C: Acceptable Use of Computer Resources and Information Systems Policy

#### 4.0 Unacceptable Use

##### *4.1 System and Network Activity*

- ✓ Violation of copyright
- ✓ Installation of software
- ✓ Using peer-to-peer file sharing services
- ✓ Revealing user account password
- ✓ Attempting to bypass controls



### C: Acceptable Use of Computer Resources and Information Systems Policy

##### *4.2 Email and Communications Activities*

- ✓ "Spamming"
- ✓ Chain and pyramid emails
- ✓ Attempting to hide sender

##### *4.3 Social Networking*

- ✓ Revealing Personal & Confidential information
- ✓ Posts that may tarnish business image
- ✓ Posting copyrighted material



## D: Password Control Policy

When do you need this Policy?

- ❖ If you allow electronic access to Personal or Confidential Information
- ✓ If you wish to control access to your Computer Resources and Information Systems

Passwords are the equivalent of physical keys to your premises from anywhere



## D: Password Control Policy

**The New York Times** January 22, 2010  
**If Your Password Is 123456, Just Make It HackMe**  
 Back at the dawn of the Web, the most popular account password was "12345."

Today, it's one digit longer but hardly safer: "123456."

Despite all the reports of Internet security breaches over the years, including

According to a new analysis, one out of five Web users still decides to leave the digital equivalent of a key under the doormat: they choose a simple, easily guessed password like "abc123," "looneyyou" or even "password" to protect their data.

"I guess it's just a genetic flaw in humans," said Aronche Shulman, the chief technology officer at Imperva, which makes software for blocking hackers. "We've been following the same patterns since the 1990s."

**MOST POPULAR PASSWORDS**  
 Nearly one million RockYou users chose these passwords to protect their accounts.

1	123456	17	michael
2	12345	18	ashley
3	123456789	19	654321
4	password	20	qwerty
5	looneyyou	21	iloveu
6	princess	22	michelle
7	rockyou	23	111111
8	1234567	24	9
9	12345678	25	ligger
10	abc123	26	password1
11	nicole	27	suzanne
12	daniel	28	chocolate
13	babygirl	29	anthony
14	monkey	30	angel
15	jessica	31	FRENCH
16	lovely	32	soccer

Source: Imperva  
 The New York Times

Mr. Shulman and his company examined a list of 32 million passwords that an unknown hacker stole last month from RockYou, a company that makes software for users of social networking sites like Facebook and MySpace. The list was briefly posted on the Web, and hackers and security researchers downloaded it. RockYou, which had already been widely criticized for lax privacy practices, has advised its customers to change their passwords, as the hacker gained information about their e-mail accounts as well.

The trove provided an unusually detailed window into computer users' password habits. Typically, only government agencies like the F.B.I. or the National Security Agency have had access to such a large password list.

"This was the mother lode," said Matt Weir, a doctoral candidate in the crime and investigation technology lab at Florida State University, where researchers are also examining the data.

Imperva found that nearly 1 percent of the 32 million people it studied had used "123456" as a password. The second-most-popular password was "12345." Others in the top 20 included "qwerty," "abc123" and "princess."

More disturbing, said Mr. Shulman, was that about 20 percent of people on the RockYou list picked from the same, relatively small pool of 5,000 passwords.



## D: Password Control Policy

### 1.0 Overview

- ❖ All Personnel and Third Parties are responsible for maintaining secure passwords

### 2.0 Purpose

- ❖ Establish standard for password content

### 3.0 Scope

- ❖ All Personnel and Third Parties who have a user account or store any information on the network



## D: Password Control Policy

### 4.0 Policy

#### 4.1 General

- ❖ Do not share accounts
- ✓ Passwords should be changed on interval and
  - ❖ *whenever an employee is terminated:*
    - User
    - Email
    - Application
    - System-level (administrators)
    - Website
    - Wireless keys
- ✓ No passwords in email



## D: Password Control Policy

---

### 4.2 Standards for not easily guessed passwords

- ✓ Minimum length
- ✓ Does not contain user name
- ✓ Complexity
  - Uppercase/Lowercase/Numbers/Special Characters
- ✓ Not a "real" word
- ✓ Not family, pets, common places or terms



## D: Password Control Policy

---

### 4.2 Standards for not compromising passwords

- ✓ Don't use the same password everywhere
- ✓ Don't reveal to anyone
  - Manager
  - Vacation help
  - Family
  - Technical help
- ✓ Don't use blatant "hints"
- ✓ Don't store in files unless encrypted
- ✓ Don't use "remember password" features



## E: Remote Access Policy

---

### When do you need this Policy?

- ❖ If you allow Personnel or Third Parties to access Personal or Confidential Information from remote locations
- ✓ If you allow Personnel or Third Parties to access your Computer Resources and Information Systems from remote locations



## E: Remote Access Policy

---

### 1.0 Purpose

- ❖ Define secure practice for working from remote locations

### 2.0 Scope

- ❖ Personnel and Third Parties using any form of remote access software
  - Remote Desktop Connection
  - GoToMyPC
  - LogMeIn
  - VNC
  - Etc...



## E: Remote Access Policy

---

### 3.0 General

- ❖ Treat Remote Access as you would treat work in the office
- ❖ If remote network is wireless, it must comply with Wireless Communications Policy



## E: Remote Access Policy

---

### 4.0 Policy

- ❖ Do not share remote access with anyone
- ✓ Use business email for all business communication
- ✓ Computers should not be connected to other networks when used for remote access
- ❖ Must run malware
- ✓ Only approved remote access solutions



## F: Wireless Communication Policy

---

### When do you need this Policy?

- ❖ If you provide a wireless network within the organization that allows access to Personal or Confidential information
- ❖ If Personnel or Third Parties using Remote Access utilize a wireless network in the remote location



## F: Wireless Communication Policy

---

### 1.0 Purpose

- ❖ Specify technical requirements for wireless devices used to connect to the network

### 2.0 Scope

- ❖ Any wireless infrastructure used to connect to the network
  - Office
  - Private (home)
  - Public (airports, internet cafes, public access points, etc.)



## **F: Wireless Communications Policy**

---

### 3.0 Policy

- ❖ All wireless used to access the organization must be encrypted
  - If in doubt, don't use the network
- ✓ Home and office wireless must:
  - Enable WPA or WEP Security
  - Disable broadcast of network name (SSID)
  - Not use default id. and password for the wireless device
  - Key change periodically and when employees are terminated



## **G: Mobile Computing and Storage Device Use Policy**

---

### When do you need this Policy?

- ❖ If you allow Personal or Confidential Information to be stored on mobile computing and storage devices



## **G: Mobile Computing and Storage Device Use Policy**

---

### 1.0 Purpose

- ❖ Mitigate the risks to Personal and Confidential electronic information carried on devices outside the local network

### 2.0 Background/History

- ✓ Portable devices are uniquely susceptible to theft
- ✓ Portable devices have been implicated in recent credit card and identity theft incidents



## **G: Mobile Computing and Storage Device Use Policy**

---

### 3.0 Scope

- ❖ Personnel and Third Parties that use laptops, tablet computers, smart phones, DVDs, CDs, memory keys and other devices that can carry electronic information

### 4.0 Policy

- ✓ Only devices approved by the Security Officer will be used by Personnel and Third Parties for Personal or Confidential Information



## G: Mobile Computing and Storage Device Use Policy

---

### 4.0 Policy

- ❖ Devices that contain Personal or Confidential Information *must be encrypted*
- ❖ If a device cannot be encrypted, it cannot be used for Personal or Confidential Information
- ✓ If a portable device is stolen or lost Personnel and Third Parties must:
  - Notify the Security Officer
  - Take all available remedies to prevent use of the device



## H: Information Retention and Destruction Policy

---

### When do you need this Policy?

- ✓ To specify how long Personal or Confidential Information (and other documents) must be retained to comply with federal and state laws and industry guidelines
- ✓ To specify procedures for destroying Personal or Confidential Information (and other documents)
- ✓ To clearly state what happens during litigation holds



## H: Information Retention and Destruction Policy

---

### 1.0 Purpose

- ✓ Ensure compliance with federal and state laws and regulations
- ✓ Eliminate accidental or innocent destruction of records
- ✓ Free up valuable storage space

### 2.0 Scope

- ✓ All Physical and Electronic records



## H: Information Retention and Destruction Policy

---

### 3.0 Document Retention

- ✓ What to retain and how long to retain it

Corporate Records	
Annual Reports to Secretary of State/Attorney General	Permanent
Articles of Incorporation	Permanent
Board Meeting and Board Committee Minutes	Permanent
Board Policies/Resolutions	Permanent
By-laws	Permanent
Construction Documents	Permanent
Fixed Asset Records	Permanent
Application for Tax-Exempt Status (Form 1023)	Permanent
Determination Letter	Permanent
State Sales Tax Exemption Letter	Permanent
Contracts (after expiration)	7 years
Correspondence (general)	3 years



## H: Information Retention and Destruction Policy

---

### 4.0 Electronic Documents and Records

- ✓ Follow the same guidelines as paper documents
- ✓ Email also follows the same guidelines

### 5.0 Emergency Planning

- ✓ Both Physical and Electronic records to be securely stored
- ✓ Electronic records to be backed up for emergency recovery purposes
- ✓ *Backup does not provide retention*



## H: Information Retention and Destruction Policy

---

### 6.0 Document Destruction

- ✓ Security Officer responsible for overseeing record destruction

### 7.0 Destruction of Electronic Documents and Records Storage Devices

- ✓ Must be permanently erased or destroyed before disposal
- ✓ Computer hard drives, flash memory drives, CDs/DVDs, etc.
- ✓ Often overlooked



## H: Information Retention and Destruction Policy

---

### 8.0 Litigation Holds

- ✓ All records, Physical and Electronic are retained until litigation ends.
- ✓ Effects both Personnel and Third Parties
- ✓ Supersedes all other retention and destruction policies



## I: Email and Messaging Retention and Destruction Policy

---

### When do you need this Policy?

- ✓ To specify how long Personal or Confidential Information (and other information) must be retained to comply with federal and state laws and industry guidelines
- ✓ To clearly state what happens during litigation holds
- ✓ If Email management has become a problem



## I: Email and Messaging Retention and Destruction Policy

### 1.0 Purpose

- ✓ Standards for classification and retention of Email and messaging
- ✓ Tie Email to the Information Retention and Destruction Policy
- ✓ Provide framework for managing storage requirements

### 2.0 Scope

- ✓ All Personnel and Third Parties using Email accounts provided by the organization



## I: Email and Messaging Retention and Destruction Policy

### 3.0 Message Classification and Retention

#### *3.1 Transitory Messages*

- ✓ Routine Communication
  - Notices about meetings or events
  - Internal requests for information
  - Announcements
  - Etc.
- ✓ Read and retain for no longer than needed



## I: Email and Messaging Retention and Destruction Policy

#### *3.2 Lasting Value Messages*

- ✓ Contents that are addressed in the Information Retention and Destruction Policy, for example
  - Payroll and Employee Tax Records
  - Employee Records
  - *Client / Customer / Donor / Member* Records
  - Legal, Insurance, and Safety Records
  - Historic Documents



## I: Email and Messaging Retention and Destruction Policy

#### *3.2 Lasting Value Messages*

- ✓ Retain in accordance with the Information Retention and Destruction Policy
- ✓ Move to dedicated storage
  - Print and file
  - Create a PDF and file appropriately
- ✓ Not to be stored in individual's Email or message files



## **I: Email and Messaging Retention and Destruction Policy**

---

### *3.3 Responsibility for Retention of Messages with Lasting Value*

- ✓ Determination by department responsible for class of records

### *3.4 General Message Management*

- ✓ Routinely :
  - Move Lasting Value messages to dedicated storage
  - Delete transitory messages
  - Empty Deleted Items and Spam/Junk folders
  - Delete older messages from Inbox, Sent Items and other folders



## **I: Email and Messaging Retention and Destruction Policy**

---

### 4.0 Backup Files

- ✓ Kept only for disaster recovery and short-term restoration

### 5.0 Litigation Holds

- ✓ All records, including Email are retained until litigation ends
- ✓ Effects both Personnel and Third Parties
- ✓ Supersedes all other retention and destruction policies



## **J: Website Security and Privacy Policy**

---

### When do you need this Policy?

- ❖ When you take online payments through your website for donations, memberships, event tickets, retail sales, etc.
- ❖ If you collect Personal or Confidential Information through your website



## **J: Website Security and Privacy Policy**

---

### 1.0 Purpose

- ✓ Define handling of information collected on website
- ✓ Required on website if accepting any online payments

### 2.0 Information Security

- ✓ Information Security Officer to monitor practices
- ✓ Access to visitor data is limited to specific individuals on need-to-know basis



## J: Website Security and Privacy Policy

---

### 3.0 Personal Information

- ✓ Only minimal information obtained – not using spyware to garner information
- ✓ Information supplied voluntarily not sold or shared
- ✓ May use information to send mailings or contact

### 4.0 Credit Card Information

- ❖ Use Secure Processing



## J: Website Security and Privacy Policy

---

### 5.0 Cookies

- ✓ Only used to provide convenient operation
  - Remember preferences
  - Keep shopping cart
  - Etc.
- ✓ Not used to obtain personal information

### 6.0 Children and Privacy

- ✓ Content appropriate for all ages

### 7.0 Links to Other Sites

- ✓ Not responsible for content on other sites



## Task List

---

### Risk Assessment

- ✓ Review with staff
- ✓ Review with accountant/bookkeeper, IT, etc.

### Review the WISP Template

- ✓ Define your security program
- ✓ Select the policies that apply and refine

### Meet with IT consultant

- ✓ What is technically feasible



## Task List

---

### Approve your WISP

- ✓ Include Board or other key players

### Train your staff

- ✓ Your WISP and proper security practices
- ✓ Shared training is possible

### The WISP can and should evolve

- ✓ It doesn't have to be perfect by March 1

