Security Awareness Training

Owner’s Manual

Version 1.0
Security Awareness Training Owner’s Manual

Table of Contents

1 COPYRIGHT .................................................................................................................................................. 5

2 WELCOME .................................................................................................................................................. 5

3 SCOPE ......................................................................................................................................................... 5

4 AUDIENCE ................................................................................................................................................. 5

  4.1 ADMINISTRATIVE PERSONNEL ........................................................................................................... 6

  4.2 ALL USERS ........................................................................................................................................... 6

5 CONTENTS .................................................................................................................................................... 6

  5.1 SAE.SWF ................................................................................................................................................ 6

  5.2 SAEXAM.SWF ....................................................................................................................................... 6

  5.3 QUIZSOUND.SWF ............................................................................................................................... 6

  5.4 QUIZ.XML .......................................................................................................................................... 6

  5.5 EMAILNOTIFICATION.ASP .................................................................................................................. 7

  5.6 LOGO.JPG .......................................................................................................................................... 7

  5.7 SAE OWNERS MANUAL.DOC .............................................................................................................. 7

6 SETUP THE SECURITY AWARENESS TRAINING .................................................................................... 7

  6.1 WEB BASED APPLICATION ................................................................................................................ 7

    6.1.1 Directory setup ............................................................................................................................... 7

7 CONFIGURE THE SECURITY AWARENESS TRAINING ........................................................................... 8

  7.1 LOGO .................................................................................................................................................. 8

  7.2 XML .................................................................................................................................................. 8

  7.3 INTRO ............................................................................................................................................. 8

  7.4 COMPANY ....................................................................................................................................... 8

  7.5 DOMAIN ...................................................................................................................................... 9

    7.5.1 The TRAINING Tag ....................................................................................................................... 9

    7.5.2 The QUESTIONNAIRE Tag ......................................................................................................... 9

  7.6 NOTES ........................................................................................................................................ 10

    7.6.1 Comments .................................................................................................................................. 11

    7.6.2 FONT ....................................................................................................................................... 11

    7.6.3 Unordered List .......................................................................................................................... 11

    7.6.4 Break ...................................................................................................................................... 11

    7.6.5 Apostrophes ............................................................................................................................ 12

8 USE THE SECURITY AWARENESS TRAINING ...................................................................................... 12

  8.1 INTRO .......................................................................................................................................... 12

  8.2 LOGIN ......................................................................................................................................... 13

  8.3 TRAINING ..................................................................................................................................... 14

  8.4 EXAM ......................................................................................................................................... 15

  8.5 COMPLETION ............................................................................................................................. 16

  8.6 EMAIL NOTIFICATION .................................................................................................................... 17

9 RESTORE THE SECURITY AWARENESS TRAINING ............................................................................. 18

  9.1 SECURITY AWARENESS TRAINING AND EXAM ........................................................................... 18

    9.1.1 Intro ...................................................................................................................................... 18

    9.1.2 Domain 1: Security Policy ...................................................................................................... 18

Secure Commerce Systems, Inc.
1 866 SEC COMM
www.securecommercesystems.com
<table>
<thead>
<tr>
<th>Domain</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.3</td>
<td>Domain 2: Organizational Security</td>
<td>19</td>
</tr>
<tr>
<td>9.1.4</td>
<td>Domain 3: Asset Classification and Control</td>
<td>22</td>
</tr>
<tr>
<td>9.1.5</td>
<td>Domain 4: Personnel Security</td>
<td>24</td>
</tr>
<tr>
<td>9.1.6</td>
<td>Domain 5: Physical and Environmental Security</td>
<td>27</td>
</tr>
<tr>
<td>9.1.7</td>
<td>Domain 6: Communications and Operations Management</td>
<td>30</td>
</tr>
<tr>
<td>9.1.8</td>
<td>Domain 7: Access Control</td>
<td>35</td>
</tr>
<tr>
<td>9.1.9</td>
<td>Domain 8: Systems Development and Maintenance</td>
<td>41</td>
</tr>
<tr>
<td>9.1.10</td>
<td>Domain 9: Business Continuity Management</td>
<td>45</td>
</tr>
<tr>
<td>9.1.11</td>
<td>Domain 10: Compliance</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>EXAM ANSWERS</td>
<td>49</td>
</tr>
<tr>
<td>11</td>
<td>SUPPORT</td>
<td>50</td>
</tr>
</tbody>
</table>
1 Copyright

All material included in the security awareness training included the training content, its related web presentation files and documentation is copyrighted by Secure Commerce Systems in the year 2003. Any distribution or reproduction of this material in whole or in part will be prosecuted. To report infringes of Secure Commerce Systems copyright, please contact us:

Secure Commerce Systems
17225 El Camino Real Suite 340
Houston, Texas 77058
1 866 SEC COMM
www.securecommercesystems.com

2 Welcome

Thank you for purchasing a flash presentation of security awareness training and exam from Secure Commerce Systems. Security awareness is vital to any organization to safeguard its enterprise from outside and inside attack. It is the first and most important step to protecting informational assets. Security awareness helps protect information and can actually prevent informational disasters from occurring.

3 Scope

The scope of this document is to introduce the security awareness training and exam to executive and administrators, so they will be able to successfully distribute the knowledge of security awareness to their organization. This document will include the following:

- What is included in the security awareness program
- How to setup the security awareness program
- How to configure the security awareness material
- How to use the security awareness training

4 Audience

The audience of the security awareness training and exam is both administrative personnel and the general user community:
Security Awareness Training Owner’s Manual

4.1 Administrative Personnel
Administrative personnel will get the most use out of the security awareness training owner’s manual, so this document is intended for administrative personnel who would configure the security awareness training and administer the exam. This material discussed herein will enable the administrator to deploy the security awareness training program.

4.2 All Users
This document is not intended for the general user community, but the security awareness training itself is intended for all personnel in an organization from top to bottom. It is vital that all users are training and certified by examination to help prevent informational loss.

5 Contents
You have most likely acquired a CD with the contents of the security awareness exam. This CD will contain all of the necessary files for you to begin rolling out the security awareness training. The following files should be found on your CD:

5.1 sae.swf
This is an intro to page to the security awareness training. This page is mostly for visual effect to grab the user’s attention and to get them interested in the security awareness training. This file is in a flash format.

5.2 saexam.swf
This is the actual exam file. The user is taken directly to this page after the intro times out or if the user chooses to select the ‘Skip Intro’ link. The user will remain on this page until the training and examination has been completed. This file is also in a flash format.

5.3 quizsound.swf
This is a music file. A catchy music file has been provided with the security training to assist in motivating the user to consume the material. The music will play once loaded on both the intro page and exam page. The music can be turned on and off at any time.

5.4 quiz.xml
This is the most important file and, as an administrator, the one with which you will most be concerned. By modifying this file, you can configure the training and exam to meet your organization’s specific needs. The exam ships in such that it will meet most organization’s needs, so configuration may not be required. This file is in an XML format.
Security Awareness Training Owner’s Manual

5.5 emailnotification.asp
This file is an ASP file and performs the function of sending email to the designated exam administrator. The email will display the results of the user’s exam, and certification can then be awarded if justified.

5.6 logo.jpg
This is an image file which is used to display the desired organization’s logo. The CD is shipped with the Secure Commerce Systems logo.

5.7 SAE Owners Manual.doc
This document.

6 Setup the security awareness training

6.1 Web based application
The security awareness program is a web-based application. You will need to have a web server commensurate with your organization designated for the security awareness training and exam. Your organization can take steps to reduce the load on your web server by administering the training and exam by department or group. Moreover, the web server must be able to support flash applications as well as active server pages. If your web server does not support these formats, the security awareness program will not work.

6.1.1 Directory setup
Once you have verified that your web server is capable of supporting the formats included in the security awareness training, you can proceed to setting up the directory. The following files must all reside in the same directory on the web server:

- sae.swf
- saexam.swf
- quizsound.swf
- quiz.xml
- emailnotification.asp
- logo.jpg

Secure Commerce Systems recommends that you use an address and directory similar to the following:

http://www.yourcompany.com/.../sae/sae.swf
Please note that sae.swf is the target file in this directory where you will direct your users to address for taking the exam.

7  Configure the security awareness training

The security awareness training and exam is configurable for your organization’s specific needs. Most of the configuration is available by manipulating the xml file: quiz.xml.

7.1  Logo

The logo.jpg will display on the login screen and throughout the exam. To change the logo from the scs logo to your company’s logo, simply remove the logo.jpg from the setup directory (described in section 5) and replace that file with your company’s logo with the same filename.

7.2  XML

Knowledge of XML is not really necessary for successful administration of the security awareness training. A rudimentary explanation of the knowledge needed will be explained in this section.

XML uses tags to delaminate sections. An XML tag will have the name of the tag surrounded by <> . The start and end of an XML tag must be noted. The closing tag is the same as the opening tag except that the closing tag’s name is preceded by /. For example the CHOICE tag is used to specify answers for exam questions. A complete CHOICE tag would be specified by:

<CHOICE>The answer is </CHOICE>

Keep this in mind as the following sections are discussed.

7.3  Intro

The INTRO tag is the first tag you may want to modify. The text in this tag is much like a written paragraph. Should you need to change this section, modify the text as needed, but do not modify the tags.

The company name of Secure Commerce Systems appears in the FONT tag. You can change this to change the company name to your company.

7.4  Company

You must configure the COMPANY tag. The COMPANY tag sets the following:
The security awareness training admin. To change the admin, change the value of EMAIL found in the COMPANY tag. Change only the value inside of the double quotes ("."). The EMAIL value will receive an email for every user who takes the exam. Make sure the value inside the double quotes is a valid email address.

- The passing grade. To change the passing grade, change only the number inside the double quotes for the PASS value inside the COMPANY tag. It is recommended that you choose a value that is at least ¾ of the total number of questions.

- The training duration. To change the duration of the exam, change only the number inside the double quotes for the TIMEOUT value inside the COMPANY tag. This is the total time for training and exam. It is recommended that it is long enough to read and understand the material and take the exam, but not too long to produce boredom on the part of the user.

- The training title. To change the title, change only the value of the text out side the > of the opening COMPANY tag and before the < of the closing COMPANY tag.

The default company tag looks like the following:

```xml
<COMPANY EMAIL="bwhite@securecommercesystems.com" PASS="25" TIMEOUT="120"> ISO 17799
</COMPANY>
```

### 7.5 Domain

The DOMAIN tag is broken down into 2 major tags: TRAINING and QUESTIONAIRE. These tags appear adjacent to each other in each domain. The General format of a DOMAIN tag is as follows:

```xml
<DOMAIN>
  <TRAINING>
  </TRAINING>
  <QUESTIONAIRE>
  </QUESTIONAIRE>
</DOMAIN>
```

The TRAINING and QUESTIONAIRE are described in greater detail below.

#### 7.5.1 The TRAINING Tag

The TRAINING tag contains the content of the security awareness training. The administrator may want to slightly modify the content to configure it to directly address the specific nature of the organization’s security policy. Other tags are found in this section. See section 6.6 for greater description.

#### 7.5.2 The QUESTIONAIRE Tag
The QUESTIONAIRE tag contains the security awareness exam questions and responses. The QUESTIONAIRE tag is made up of two other tags: QUESTION and CHOICE. The QUESTIONAIRE tag has the following general format:

```xml
<QUESTIONAIRE>
  <QUESTION>
    <CHOICE></CHOICE>
    <CHOICE></CHOICE>
    <CHOICE></CHOICE>
  </QUESTION>
</QUESTIONAIRE>
```

The QUESTION and CHOICE tags are described in greater detail below.

7.5.2.1 The QUESTION tag

The QUESTION tag has two parameters: TEXT and ANSWER. Both of values of these parameters are enclosed in double quotes. The value of the TEXT parameter contains the actual question text. The value of the ANSWER parameter contains the answer of the answer. The value of the ANSWER parameter correspond to the CHOICE tag described below. An example a QUESTION is:

```xml
<QUESTION TEXT="What do I do if I suspect an incident?" ANSWER="2">
  <CHOICE>Nothing. This is for your own protection, as your actions might be interpreted as a potential misuse of the system.</CHOICE>
  <CHOICE>You must attempt to prove or fix a suspected weakness.</CHOICE>
  <CHOICE>You will report Incidents affecting security through appropriate management channels as quickly as possible.</CHOICE>
  <CHOICE>Blackmail the person responsible.</CHOICE>
</QUESTION>
```

7.5.2.2 The CHOICE tag

The CHOICE tag provides several possible choices of a correct answer for test takers. There must be only one correct CHOICE per QUESTION. Which CHOICE is correct determines the value of the ANSWER parameter in the QUESTION tag above. The value of ANSWER is enumerated based on the CHOICE tag. The CHOICE tags starts at 0 and increase by 1 for each choice included. There is no limit on choices. However, it is recommended that that there be between 2 and 5 choices.

7.6 Notes

You will find a few other tags inserted in the quiz.xml file. A Brief description of some of these other tags should make editing the file easier to understand:
7.6.1 Comments

Comments do not actually affect the output of the XML code. They are strictly added for ease of use and readability. A comment is enclosed in the following:

<!-- -->

An example of a comment in the quiz.xml file is:

<!-- Introduction -->

7.6.2 FONT

The FONT tag changes the properties of the text inside the FONT tag. In the quiz.xml file, the FONT tag is generally used to create larger text for emphasis. An example of a FONT tag is:

<font size="+2">Secure Commerce Systems</font>

The value of the size parameter inside the FONT tag determines how large the text will be.

7.6.3 Unordered List

The unordered list <UL> is used to generate just that. It creates a bulleted, indented list. Each item in the list is denoted by the list item tag <LI>. An example of such a list is:

You must be aware that the risks associated with equipment include the following and report any of these risks to your supervisor:

<ul>
  <li>Theft</li>
  <li>Fire</li>
  <li>Explosives</li>
  <li>Smoke; water (or supply failure)</li>
  <li>Dust</li>
  <li>Vibration</li>
  <li>Chemical effects</li>
  <li>Electrical supply interference</li>
  <li>Electromagnetic radiation</li>
  <li>Improper temperature or environmental conditions</li>
</ul>

7.6.4 Break

The break tag <BR> is used to add a new line to the display of the document. This is generally used in the quiz.xml file after an unordered list. See example above for usage.
7.6.5 Apostrophes

XML cannot display an apostrophe as it would normally be struck from the keyboard (‘). In order to display an apostrophe, the following must be used:

&apos;

An example of such a usage is:

You must follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user’s identity and thus to establish access rights to information processing facilities or services.

The same is true for single quote usage.

8 Use the security awareness training

8.1 Intro

Users will need to open up their browser and point the address setup by the administrator (see section 5). After the page finishes its initial load, the user will see a screen similar to the scene below.
Text will scroll on and off the screen for a few minutes with various security awareness information.

Notice the two buttons (links) on the bottom left and bottom right of the screen. The button on the bottom right turns music on and off. Music by default is set to play. However, the music file is large and may take a few seconds to load. The time will depend on the speed of your connection. The button on the bottom left will skip the intro if clicked and take you directly to the training and exam. After a few minutes, the intro will timeout and directly take you to the training.

8.2 Login
After the intro has completed, you will appear at the login screen. This is not a true login in screen where you will be authenticated. The login is only necessary that the email generated by the software will be sent to an email address. The login screen is accompanied by a welcome statement to further explain a little about the material and exam. On the login screen, the user will be able to see how much time is allowed for the training and exam as well as how many questions must be correctly answered for a passing grade. This information exists centered on
Security Awareness Training Owner’s Manual

the bottom of the screen. A clock and a timer exist on the top right portion of the screen and will remain throughout the training and exam.

Music controls exist on the bottom right portion of the screen but are controlled by two buttons for stop and play. Once again, the music is defaulted to on and will start once loaded. The music will reload at the login screen and play throughout the training and exam unless stopped.

The user must enter his email and reenter it to verify it was entered consistently. Once this has been done, the user can click the “Start Quiz” button to start the training. At this point, the timer will start.

8.3 Training
The training and exam is interleaved. The user will read material for one of the 10 domains, and then start the exam for that domain. This process is repeated until the exam has been completed. Some domains contain more material than other domains. The user must use the scroll buttons on the right side of the screen to review all of the material.
After the user has read and understood all of the material from a given domain, he can select the “Start” button to begin the exam.

8.4 Exam

The user will read and answer each question for the domain one at a time. Once the user has determined his answer, using the mouse, he selects the appropriate choice. This action will take him to the next question. If a user does not wish to answer a question, he may choose the “Next” button. After completing all of the questions for a given domain, the next domain will begin immediately.
8.5 Completion
Once the user has completed the exam, he will be notified of his result, pass or fail. He will also be notified that an email has been sent to the designated administrator.
8.6 Email notification

An email notification will be sent to the designated administrator as well as to the email provided in the login screen. It is vital that users enter a valid email during the login so that the administrator can verify that all users have undergone training and that certifications can be awarded. The email will have the following format:

Security Awareness Exam

Taken By: bwhite@securecommercesystems.com
Date: 1/22/2004
Score: 1/33
Result: Sorry, you've failed the exam.

Missed Questions:
...

Security Awareness Training Owner’s Manual

Secure Commerce Systems, Inc.
1 866 SEC COMM
www.securecommercesystems.com
9 Restore the security awareness training

Because our security awareness program is highly configurable, please retain the CD and this document to restore to the original configuration if you damage your production version. The original content of the training and exam exist on the CD in quiz.xml and appears below for your reference.

9.1 Security Awareness training and exam

9.1.1 Intro

Welcome to the Secure Commerce Systems security awareness training course. This course will highlight the ten domains or sections of the ISO 17799 security policy and discuss your responsibilities as a result of the policy. You are responsible for understanding and complying with the security policy. Failure to do so will result in corrective action and may result in termination.

This presentation will give you information in the basics of security awareness and help you to meet your responsibilities to the security policy. You will be required to take an examination on material discussed in the security awareness training course. Your supervisor will be notified of your examination results.

9.1.2 Domain 1: Security Policy

Your company has set a clear policy direction and demonstrates support for, and commitment to, information security through the issue and maintenance of an information security policy across your company.

This policy and related procedures apply to all users of the company information systems, including employees, contractors, consultants, temporary workers and business partners. You are responsible for adhering to the policy and related procedures.

The policy will include:

- A definition of information security, its overall objectives and the responsibilities and expectations for security management of assets managed by your company.
- A brief explanation of the security policies, procedures, standards and compliance requirements of particular importance to your company.
- A definition of general responsibilities for information security management.
- References to documentation, which may support the policy; e.g. more detailed security policies and procedures for specific information systems or security rules with which users must comply.
9.1.2.1  Question 1: What is the purpose of the security policy?
   a) Your company has established a security policy to satisfy federal security requirements.
   b) Your company has set a security policy to provide a safe environment in which to work.
   c) Your company has set a security policy to bore you to tears.
   d) Your company has set a clear policy direction and demonstrates support for, and commitment to, information security through the issue and maintenance of an information security policy across your company.

9.1.2.2  Question 2: The policy and related procedures apply to all users of the company information systems, including employees, contractors, consultants, temporary workers and business partners.
   a) True
   b) False

9.1.3  Domain 2: Organizational Security

A multi-disciplinary approach to information security will be incorporated, which involves the cooperation and collaboration of managers, users, administrators, application designers, and security staff.

Management Information Security Forum

Information security is a business responsibility shared by all members of the management team. A management forum will promote security within the organization through appropriate commitment and adequate resourcing.

The forum is tasked with the responsibility of maintaining the security policy, keeping it up to date and a viable solution in the protection of information at your company.

You are responsible for making yourself aware of potential vulnerabilities that are not yet addressed and reporting them to your Computer Information Security Officer or designated security supervisor so that the issue can be addressed and the vulnerability mitigated.

The security policy is a living and breathing document and needs your diligence to protect yourself and the city.

Information Security Coordination

In a large organization a cross-functional forum of management representatives from relevant parts of the organization will be established to co-ordinate the implementation of information security controls.

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators will be maintained to ensure that appropriate action
Security Awareness Training Owner’s Manual

can be quickly taken, and advice obtained, in the event of a security incident. Similarly, membership of security groups and industry forums will be established.

Exchanges of security information will be restricted to ensure that confidential information of the organization is not passed to unauthorized persons

You are responsible in cooperating with other personnel in communicating and enforcing security controls.

Allocation of Information Security Responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes will be clearly defined.

- The various assets and security processes associated with each individual system will be identified and clearly defined.
- The manager responsible for each asset or security process will be agreed and the details of this responsibility will be documented.
- Authorization levels will be clearly defined and documented.

Security is your responsibility! If you have access to and asset either physically or electronically, you are responsible for keeping that asset secure. If you think an asset may be compromised, you must report it immediately.

Authorization Process for Information Processing Facilities

A management authorization process for new information processing facilities will be established. The following controls will be implemented:

- New facilities will have appropriate user management approval, authorizing their purpose and use. Approval will also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met.
- Where necessary, hardware and software will be checked to ensure that they are compatible with other system components.
- The use of personal information processing facilities for processing business information and any necessary controls will be authorized.
- The use of personal information processing facilities in the workplace may cause new vulnerabilities and will therefore be assessed and authorized.

You are responsible for using only authorized facilities. If you need access to unauthorized facilities, you must gain authorization for that facility.

Specialist Information Security Advice
Specialist security advice is likely to be required from time-to-time. The Computer Information Security Officer will also have access to suitable external advisers to provide specialist advice outside his or her own experience.

The information security adviser or equivalent point of contact should be consulted at the earliest possible stage following a suspected security incident or breach to provide a source of expert guidance or investigative resources.

If you detect a security breach of any kind or have any information regarding a security incident, you must report that information.

**Security of Third Party Access**

When a definitive business need exists for third party access, a risk assessment will be carried out to determine security implications and control requirements. Controls are defined in a contract with the third party at-hand.

**Types of Access**

The risks of access across a network connection are different from risks resulting from physical access. Therefore, the types of access that will be addressed are:

- Physical access, e.g. to offices, data centers, filing cabinets.
- Logical access, e.g. to your company’s databases, information systems.

**On-Site Contractors**

Third parties that are located on-site for a period of time (as defined in their contract) may also give rise to security weaknesses. Arrangements involving third party access to your company information systems will be based on a formal contract.

You are responsible for cooperating with third parties as the need arises, but at the same time acting as a security watchdog to ensure that third parties do not gain access to areas to which they do not have access and are not endangering your company’s intellectual property.

9.1.3.1 **Question 3: What does the Management Information Security Forum do?**

a) The forum is tasked with the responsibility of creating the security policy.

b) The forum is tasked with the responsibility of maintaining the security policy, keeping it up to date and a viable solution in the protection of information at your company.

c) The forum is tasked with the responsibility of educating your company personnel of security policy procedures.

d) The forum is tasked with the responsibility of investigating security breaches and initiating prosecution against policy violators.
9.1.3.2  **Question 4: What is my role regarding the Management Information Security Forum?**  
   a) You are responsible for making yourself aware of potential vulnerabilities that are not yet addressed and reporting them to your Computer Information Security Officer or designated security supervisor so that the issue can be addressed and the vulnerability mitigated.
   b) You are responsible for monitoring other personnel including employees, contractors, consultants, temporary workers, business partners and management and investigating suspicious activity to prevent a breach of asset security.
   c) You are responsible in cooperating with other personnel in communicating and enforcing security controls. Security is your responsibility! If you have access to and asset either physically or electronically, you are responsible for keeping that asset secure. If you think an asset may be compromised, you must report it immediately.
   d) A and C.
   e) All of the above.

9.1.3.3  **Question 5: Which of the following is not a type of access?**  
   a) Physical access.
   b) Remote access.
   c) Logical access.

9.1.3.4  **Question 6: How should I work with contractors and other third party personnel?**  
   a) You are responsible for cooperating with third parties as the need arises since they have been brought in by management for a specific need and do not pose a security threat since they only have temporary access to your company’s intellectual property.
   b) You are responsible for protecting the company information security. Contractors and third party personnel do not have the right to access your company’s intellectual property. Cooperating with third parties is a risk to company information security and you are responsible for acting as a security watchdog.
   c) You are responsible for cooperating with third parties as the need arises, but at the same time acting as a security watchdog to ensure that third parties do not gain access to areas to which they do not have access and are not endangering your company’s intellectual property.
   d) You are responsible for ignoring them unless they take you to lunch.

9.1.4  **Domain 3: Asset Classification and Control**

**Accountability for Assets**

All major information assets will be accounted for and have a nominated owner.

Owners will be identified for all critical assets and the responsibility for the implementation and maintenance of appropriate controls is assigned to ensure that appropriate protection is being used. Responsibility for implementing controls may be delegated. Ultimate responsibility will remain with the company owner of the asset.
Inventory of Assets

Inventories of assets help ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important aspect of risk management.

An inventory must be maintained of the important assets associated with each information system. Each asset will be clearly identified and its ownership and security classification agreed and documented, together with its current location (important when attempting to recover from loss or damage). Examples of assets associated with information systems are:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information.
- Software assets: application software, system software, development tools and utilities.
- Physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air conditioning units), furniture, accommodation.
- Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

You are responsible for helping to maintain asset inventories. If assets are added, removed or moved you must notify appropriate personnel to update asset inventories.

Information Classification

Information will be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system will be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

You are responsible for adhering to the classification of information and the appropriate handling thereof.

Information Labeling and Handling

For each classification, handling procedures must be defined to cover the following types of information processing activity:

- Copying.
- Storage.
- Transmission by post, fax, and electronic mail.
- Transmission by spoken word, including mobile phone, voicemail, answering machines.
You are responsible for maintaining the integrity of information in your charge in any state of information processing listed above. Following classification labels will help you maintain that integrity.

9.1.4.1 Question 7: Which of the following is not an example of assets associated with information systems?
   a) Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information.
   b) Software assets: application software, system software, development tools and utilities.
   c) Physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air conditioning units), furniture, accommodation.
   d) Transportation assets: Equipment used in transportation, e.g. company vehicles, construction equipment, public transportation.
   e) Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

9.1.4.2 Question 8: How will assets be classified?
   a) Information will be classified to indicate the need, priorities and degree of protection.
   b) Information will be classified by the monetary cost of the asset.
   c) Information will be classified by department.
   d) Information will be classified with post-it notes.

9.1.4.3 Question 9: You are responsible for maintaining the integrity of information in your charge in any state of information processing listed above. Following classification labels will help you maintain that integrity.
   a) True
   b) False

9.1.5 Domain 4: Personnel Security

Security in Job Definition and Personnel Management

Security responsibilities will be addressed at the recruitment stage, included in contracts, and monitored during an individual’s employment. All employees and third party users of information processing facilities must sign a confidentiality (non-disclosure) agreement. If you have not signed such an agreement, you must inform your supervisor immediately.

Including Security in Job Responsibilities
Security Awareness Training Owner’s Manual

Security roles and responsibilities will be documented where appropriate. They will include any
general responsibilities for implementing or maintaining security policy as well as any specific
responsibilities for the protection of particular assets, or for the execution of particular security
processes or activities.

Personnel Screening and Policy

Verification checks on permanent staff will be carried out at the time of job applications and or
promotions. This will include the following controls:

- Availability of satisfactory character references, e.g. one business and one personal.
- A check (for completeness and accuracy) of the applicant’s curriculum vitae.
- Confirmation of claimed academic and professional qualifications.
- Independent identity check (passport or similar document).
- Credit Check when necessary.

You will be subject to periodic review and approval procedures by a more senior member of
staff.

Terms and Conditions of Employment

Your responsibility for information security is part of the terms and conditions of employment.
When appropriate, these responsibilities will continue outside the organization’s premises and
for a defined period after end of your employment with the city. The action to be taken if you
disregard security requirements will be included.

User Training

You will be trained in security procedures and the correct use of information processing facilities
to minimize possible security risks with courses similar to this. You will be made aware of the
risks, how they arise, and how to mitigate the risks in the course of a normal business day.

Responding to Security Incidents

You will report Incidents affecting security through appropriate management channels as quickly
as possible. All employees and contractors will be made aware of the procedures for reporting
the different types of incident (security breach, threat, weakness or malfunction) that might have
an impact on the security of organizational assets. The organization will establish a formal
disciplinary process for dealing with employees who commit security breaches. To be able to
address incidents properly it might be necessary to collect evidence as soon as possible after the
occurrence.
Employees who deliberately violate the information security policy or related documentation may be subject to disciplinary action up to and including termination. Your company requires that 3rd party contract firms take appropriate action for their employees who violate the information security policy. Your company reserves the right to deny contract employees access to company facilities and systems as deemed necessary to protect information.

**Reporting Security Weaknesses**

As a user of information services, you are required to note and report any observed or suspected security weaknesses in, or threats to, systems or services. You should report these matters either to their management or directly to their service provider as quickly as possible. However, you must not, under any circumstances, attempt to prove a suspected weakness. This is for your own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

**Reporting Software Malfunction**

Procedures will be established for reporting software malfunctions. The following actions will be established:

- The symptoms of the problem and any messages appearing on the screen will be noted.
- The computer will be isolated, if possible, and use of it will be stopped. The appropriate contact will be alerted immediately. If equipment is to be examined, it will be disconnected from any organizational networks before being re-powered. Diskettes will not be transferred to other computers.

You must immediately report the matter to the information security manager. You will not attempt to remove the suspected software unless authorized to do so. Appropriately trained and experienced staff will carry out recovery.

**Disciplinary Process**

There will be a formal disciplinary process for employees who have violated organizational security policies, and such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. Additionally, it should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.

9.1.5.1 Question 10: Security roles and responsibilities include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

a) False  
b) True
9.1.5.2 Question 11: How does the company control who is hired?
   a) Verification checks on permanent staff will be carried out at the time of job applications and or promotions.
   b) You will be subject to periodic review and approval procedures by a more senior member of staff.
   c) Random criminal background checks are performed and those with criminal histories are not considered.
   d) A and B
   e) A and C

9.1.5.3 Question 12: What do I do if I suspect an incident?
   a) Nothing. This is for your own protection, as your actions might be interpreted as a potential misuse of the system.
   b) You must attempt to prove or fix a suspected weakness.
   c) You will report Incidents affecting security through appropriate management channels as quickly as possible.
   d) Blackmail the person responsible.

9.1.6 Domain 5: Physical and Environmental security

Physical Security Perimeter

Your company will use security perimeters to protect areas that contain information processing facilities. A security perimeter is something that builds a barrier, e.g. a wall, a card controlled entry gate or a manned reception desk. The position and strength of each barrier depends on the results of a risk assessment.

Only authorized personnel are allowed access to security areas, so you must refrain from areas from which you do not have access. You are responsible for maintaining the integrity of security perimeter. If you become aware of unauthorized personnel in a security perimeter or a vulnerability to a security perimeter, you must report the incident to the appropriate security supervisor.

Physical Entry Controls

Secure areas will be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Controls that are directly related to your diligence include:

- Visitors to secure areas will be supervised or cleared and their date and time of entry and departure recorded. They will only be granted access for specific, authorized purposes and will be issued with instructions on the security requirements of the area and on emergency procedures. You will be required to wear some form of visible identification and will be required to challenge unescorted strangers and anyone not wearing visible identification.

- Access to sensitive information and information processing facilities, will be controlled and restricted to authorized persons only. Authentication controls, e.g. swipe card plus PIN, will be used to authorize and
Security Awareness Training Owner’s Manual

validate all access. An audit trail of all access will be securely maintained. You must carefully guard keys and other access devices to offices or secure areas.

- Photographic, video, audio or other recording equipment will not be allowed, unless authorized. You are responsible for reporting unauthorized devices.

Isolated Delivery and Loading Areas

Delivery and loading areas are a potential point of attack and will be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. If you have access to a delivery or loading area you must be aware and enforce the following controls:

- Access to a holding area from outside of the building will be restricted to identified and authorized personnel, and you must report unauthorized personnel.

- The holding area will be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building. If you are aware of delivery staff leaving designated areas, you must report the incident to the appropriate security supervisor.

- The external door(s) of a holding area will be secured when the internal door is opened. You must see that the appropriate door is closed and the incident is reported.

- Incoming material will be inspected for potential hazards before it is moved from the holding area to the point of use. You must report uninspected potentially hazardous material to your appropriate security supervisor.

Equipment Security

Security is not solely achieved by protecting from outside or inside attack. Safety is inexorably linked to security. In order to be secure, you must be safe as well. This is particularly true in the use of equipment. You must help insure that equipment which you use or with which you come in contact are physically protected from security threats and environmental hazards.

You must be aware that the risks associated with equipment include the following and report any of these risks to your supervisor:

- Theft
- Fire
- Explosives
- Smoke; water (or supply failure)
- Dust
- Vibration
- Chemical effects
- Electrical supply interference
- Electromagnetic radiation
- Improper temperature or environmental conditions
Your company holds you equally responsible for maintaining equipment security. You are responsible to stop ‘shoulder surfing’. Shoulder surfing is overlooking someone else’s shoulder during the use of sensitive data. You also prohibited from eating, drinking or smoking in data center. You must also use protection devices such as keyboard membranes for equipment in industrial environments.

Other areas of equipment risk include power supplies, cabling and lapses in scheduled maintenance by authorized personnel. If you notice suspicious or faulty equipment at these points, you must report the incident. Eventually equipment or media will need to be removed or reused. If you are involved in the disposal or re-use of equipment or media, you must securely remove all sensitive data.

**Security of Equipment Off-Premises**

Sometimes it becomes necessary to use equipment off-premises. If you need to use equipment or media off-premises, regardless of ownership, you must obtain authorization.

The following guidelines will be utilized:

- You must not leave equipment and media taken off the premises unattended in public places. Portable computers must not be left in a visible public place when unattended (e.g. front or back seat of a car).
- You must follow manufacturers’ instructions for protecting equipment at all times.
- You must have adequate insurance coverage to protect equipment off site.
- You must use common sense with equipment off site.

**General Controls**

To reduce the risks of unauthorized access or loss, your company has adopted a clear screen and clear desk policy. You are responsible for the following controls:

The following controls will be implemented:

- You must securely store paper and computer media containing sensitive or critical business information in suitable locked cabinets or other secure storage apparatus.
- You must lock or log off personal computers and computer terminals and printers when not in use.
- You must immediately clear sensitive or classified information when printed.

**9.1.6.1 Question 13: Which of the following are examples of a security perimeter?**

a) Controlled entry gate.

b) Manned reception desk.

c) Wall.

d) All of the above.
9.1.6.2 Question 14: What is not my responsibility with respect to security perimeters?
   a) You will be required to wear some form of visible identification and will be required to
      challenge unescorted strangers and anyone not wearing visible identification.
   b) After providing adequate authentication, you must log your entrance to a security
      perimeter.
   c) You must carefully guard keys and other access devices to offices or secure areas.
   d) You are responsible for reporting unauthorized devices such as cameras.

9.1.6.3 Question 15: Which is not a risk associated with internal physical security?
   a) Smoke.
   b) Vibration.
   c) Noise.
   d) Theft.

9.1.6.4 Question 16: Which of the following are prohibited when taking company assets
   (equipment or media off-premises, regardless of ownership) off-site?
   a) Getting authorization for taking assets off-site.
   b) Having insurance coverage for taking assets off-site.
   c) Following manufacturers’ instructions while using assets off-site.
   d) Leaving equipment unattended in a public area while using assets off-site.

9.1.6.5 Question 17: What is not part of the clear-screen policy?
   a) You must clean dust off the monitor screen with an cleaning cloth approved by the
      manufacturer.
   b) You must securely store paper and computer media containing sensitive or critical
      business information in suitable locked cabinets or other secure storage apparatus.
   c) You must lock or log off personal computers and computer terminals and printers when
      not in use.
   d) You must immediately clear sensitive or classified information when printed.

9.1.7 Domain 6: Communications and Operations Management

Documented Operating Procedures

The operating procedures identified by the security policy will be documented and maintained.
Operating procedures will be treated as formal documents and changes authorized by
management. When applicable, you will be required to follow these procedures. By following
these procedures you will be able:
   ▪ To properly process and handle information.
   ▪ To handle errors and other exceptional conditions, which might arise during job execution, including restrictions
     on the use of system utilities.
   ▪ To know appropriate support contacts in the event of unexpected operational or technical difficulties.
- To properly handle confidential output, including procedures for secure disposal of output from failed jobs.
- To properly handle system restart and recovery procedures for use in the event of system failure.

**Operational Change Control**

Formal management responsibilities and procedures will be implemented to ensure satisfactory control of all changes to equipment, software or procedures. Operational programs will be subject to strict change control. You will be required to follow operational change control procedures and to report misapplications of change control procedures.

**Incident Management Procedures**

Incident management responsibilities and procedures will be established and a Computer Incident Response Team (CIRT) will be created to ensure a quick, effective and orderly response to security incidents. You will be required to follow incident management procedures. These procedures will cover the types of security incidents, contingency plans, investigation of incidents and recovery from incidents.

**Other Operational Procedures**

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separation of the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, will be established.

Separating development, test and operational facilities is important to achieve segregation of the roles involved. Your company has defined rules for the transfer of software from development to operational status. A level of separation will be maintained between operational, test and development environments.

Logging must be performed. If you are an operator, you will be required to keep operator logs, and all users are required to log faults in a fault log.

**System Acceptance**

Acceptance criteria for new information systems, upgrades and new versions will be established and suitable tests of the system carried out prior to acceptance. Before you accept use of a new system, you should inform yourself of the security related to the new system.

**Protection Against Malicious Software**

Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan and logic bombs.
Security Awareness Training Owner’s Manual

You will be made aware of the dangers of unauthorized or malicious software, and managers will, where appropriate, introduce special controls to detect or prevent its introduction. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers.

Here are some steps you can take to guard against malicious software:

- You cannot use unauthorized software.
- You cannot obtain files and software either from or via external networks, or on any other medium.
- You must inspect and make sure of anti-virus detection and repair software is installed and up to date on any machine in your use.
- You must report the presence of unapproved files on any machine in your use.
- You must verify emails and other such electronic media of uncertain or unauthorized origin for viruses before use.
- You must follow any special instruction handed down for particular attacks virus or otherwise. Never assume a possible attack is a hoax.
- You must make backups when appropriate and necessary.

Network Management

You must be careful to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems.

Media Handling and Security

Media will be controlled and physically protected. Appropriate operating procedures are established to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorized access. You are responsible for caring and securing these media while in your charge. You can use the following guidelines to help you safeguard media:

- You must securely erase the previous contents of any re-usable media if no longer required.
- You must obtain authorization for all media removed from the organization and a record of all such removals to maintain an audit trail will be kept.
- You must store all media in a safe, secure environment, in accordance with manufacturers’ specifications.
- You must properly and securely dispose of media that is no longer needed. You may need to receive authorization prior to final disposition.
- You must distribute media with sensitive data to only those who have need and authorization to have such media.
- You must lock sensitive data.
- You must appropriately label media.
- You must immediately report loss of data.
Security Awareness Training Owner’s Manual

Security of Media in Transit

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. If you must transport media you can help safeguard the media by using the following controls:

- You must use reliable transport or couriers. A list of authorized couriers will be agreed with management and a procedure to check the identification of couriers implemented.
- You must appropriately package the media to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers’ specifications.
- You must deliver by hand, use locked containers, tamper evident packaging, etc when necessary.
- You must use digital signatures and confidentiality encryption when appropriate.

Electronic Commerce Security

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and online transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls will be applied to protect electronic commerce from such threats, including the following:

- Authentication. The term Authentication refers to the process of validating digital certificates during the establishment of a Secure Socket Layer (SSL) session between a sending party (the client) and a receiving party (the server). As a member of the company network, you function in the role of client when sending documents and server when receiving documents.
- Server Authentication. An SSL session requires the receiving party (the server) to be authenticated by the sending party (the client) prior to transmitting the document. This authentication step requires a ‘yes’ answer to three questions:
  - Is today’s date within the validity period of the server’s certificate?
  - Is the issuing CA (Certifying Authority) a trusted CA by the client?
  - Does the issuing CA’s public key validate the issuer’s digital signature on the server’s certificate?
- Client Authentication. Client authentication requires the sending party (the client) to be authenticated by the receiving party (the server) prior to transmitting the document. Client Authentication requires a ‘yes’ answer to the same three questions asked during Server Authentication. Additionally, Client Authentication requires that the client’s public key validate the client’s digital signature.
- Signature Authentication. Digital signatures are used to verify document integrity and authenticity.

Publicly Available Systems
You must take care when dealing with information on a public system, especially that information which is sensitive. You must not put information on a public system unless it is approved and has appropriate security and legal safeguards.

Other forms of information exchange pose risks too. These systems include the telephones, facsimile machines, conversation, etc. Here are a few guidelines while in public or using public systems:

- You must not reveal sensitive information so as to avoid being overheard or intercepted when making a phone call.
- You must not have confidential conversations in public places or open offices and meeting places with thin walls.
- You must not leave messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing.

9.1.7.1 Question 18: What do I do if I suspect a system failure?
   a) Take the device to a repair facility approved by the manufacturer.
   b) Attempt to fix the system yourself.
   c) Report the problem, do not try to fix it unless authorized to do so.
   d) Let someone else handle it.

9.1.7.2 Question 19: A Computer Incident Response Team (CIRT) will be created to ensure a quick, effective and orderly response to security incidents.
   a) False.
   b) True.

9.1.7.3 Question 20: What precautions are not required to prevent and detect the introduction of malicious software?
   a) You must make backups when appropriate and necessary.
   b) You must inspect and make sure of anti-virus detection and repair software is installed and up to date on any machine in your use.
   c) You must print email attachments instead of saving them to disk.
   d) You must report the presence of unapproved files on any machine in your use.
   e) You cannot use unauthorized software.

9.1.7.4 Question 21: Which of the following guidelines is not a media handling responsibility?
   a) You must lock sensitive data.
   b) You must destroy all old data.
   c) You must securely erase the previous contents of any re-usable media if no longer required.
   d) You must distribute media with sensitive data to only those who have need and authorization to have such media.
   e) You must store all media in a safe, secure environment, in accordance with manufacturers’ specifications.
9.1.7.5 Question 22: Which of the following guidelines does not apply to publicly available systems?
   a) You must not reveal sensitive information so as to avoid being overheard or intercepted when making a phone call.
   b) You must not have confidential conversations in public places or open offices and meeting places with thin walls.
   c) You must store your password on a publicly available system just in case you forget it.
   d) You must not leave messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing.

9.1.8 Domain 7: Access Control

Access Control Rules

Access control rules and rights for each user or group of users are clearly stated in an access policy statement. Access control rules will help you operate on the premise ‘What must be generally forbidden unless expressly permitted’ rather than the weaker rule ‘Everything is generally permitted unless expressly forbidden’.

User Registration

Your company has established a formal user registration and de-registration procedure for granting access to all multi-user information systems and services which includes the following impact to your use of these systems:

- You will use a unique user ID so that you can be linked to and made responsible for your actions.
- Checking that you have authorization from the system owner for the use of the information system or service.
- You will only have access that is consistent with your business purpose.
- You will not be granted access until authorization procedures have been completed.
- A record will be kept when you are registered to use the service.
- You access will be removed immediately after you have changed jobs or left the organization.

Privilege Management

The allocation and use of privileges will be restricted and controlled. If you require privileged use, you must undergo an authorization process, and you will be allocated privileges on a need-to-use basis and on an event-by-event basis, i.e. the minimum requirement for your functional role only when needed.

User Password Management
Passwords will be assigned by your company and communicated to you via telephone. Future procedures will enable you to manage their own passwords. You must follow the following password rules:

- Your password must have an eight character minimum length.
- You password must contain at least one number, one upper case letter, and one lower case letter.
- You will be given an initial password and will be forced to change it when the first log into the system.

**Review of User Access Rights**

To maintain effective control over access to data and information services, management will conduct a formal process at regular intervals to review your access rights so that:

- Your access rights are reviewed at 6 month intervals.
- Your special privileged access rights are reviewed at 3 month intervals.

**Password Use**

You must follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user’s identity and thus to establish access rights to information processing facilities or services. You are advised to do the following:

- You must keep passwords confidential.
- You must avoid keeping a paper record of passwords, unless this can be stored securely.
- You must change your password whenever there is any indication of possible system or password compromise.
- You must select quality passwords with a minimum length of eight characters which are:
  - Easy to remember.
  - Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.
  - Free of consecutive identical characters or all-numeric or all-alphabetical groups.
- You must change temporary passwords at the first log-on and change passwords at regular intervals.
- You must not include passwords in any automated log-on process, e.g. stored in a macro or function key.
- You must not share individual user passwords.

**Unattended User Equipment**

You will ensure that unattended equipment has appropriate protection. You are advised to do the following:

- You must terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver.
- You must log-off mainframe computers when the session is finished (i.e. not just switch off the PC or terminal).
You must secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

Policy on Use of Network Services

You will only be provided with direct access to the services that they have been specifically authorized to use. A policy will be formulated concerning the use of networks and network services.

User Authentication for External Connections

External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. Therefore if you are a remote user, you will be subject to authentication. There are different types of authentication methods, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication.

Network Connection Control

Access control policy requirements for shared networks, especially those extending across organizational boundaries, may require the incorporation of controls to restrict your connection capability for application such as e-mail, file transfer, etc.

Operating System Access Control

Access to the operating systems on the production servers is only granted to company employees and their authorized representatives. Client access to the OS level for production systems is prohibited.

Automatic Terminal Identification

Automatic terminal identification will be considered to authenticate connections to specific locations and to portable equipment. Automatic terminal identification is a technique that can be used if it is important that the session can only be initiated from a particular location or computer terminal.

Terminal Log-On Procedures

The log-on procedure will disclose the minimum of information about the system, in order to avoid providing an unauthorized user with unnecessary assistance. Therefore, you must be aware of the following:

- You will not have access to application identifiers or help messages until the log-on process has been successfully completed.
Security Awareness Training Owner’s Manual

- You will be warned by a general notice warning that the computer should only be accessed by authorized users and will be prosecuted if you are unauthorized.
- You will be limited in the number of unsuccessful log-on attempts allowed (three is recommended). Upon unsuccessful attempt, you will not be notified what caused the login failure.
- You will be limited by the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.

User Identification and Authentication

You will have a unique identifier (user ID) for their personal and sole use so you’re your activities can subsequently be traced. Your user ID will not give any indication of your privilege level, e.g. manager, supervisor. Your user ID will be authenticated by password, but may more securely be authenticated with addition of tokens or smart cards, etc.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management and the Computer Information Security Officer will be documented for such cases. Additional controls may be required to maintain accountability. You must use shared ID solely for purposes and at the times intended.

Use of System Utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. Their use is restricted and tightly controlled. You will be required to authenticate to use such tools and such actions will be logged for auditing. You must refrain from inappropriately using these system utilities.

Terminal Time-out

Inactive terminals in high-risk locations, e.g. public or external areas outside the organization’s security management, or serving high-risk systems, will shut down after a defined period of inactivity to prevent access by unauthorized persons. However, do not rely on terminal time-out. It is always safer for you to lock a terminal.

Limitation of Connection Time

You will be restricted in connection times, for restrictions on connection times provide additional security for high-risk applications. Limiting the period during which terminal connections are allowed to computer services reduces the window of opportunity for unauthorized access.

Application Access Control
You will be affected by certain types of application access control. Security facilities will be used to restrict access within application systems. Logical access to software and information will be restricted to authorized users.

**Sensitive System Isolation**

Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity may indicate that the application system should run on a dedicated computer, should only share resources with trusted applications systems, or have no limitations.

**Monitoring System Access and Use**

Your access to systems will be monitored to detect deviation from access control policy and monitorable events are recorded to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model to be verified.

**Event Logging**

Your security-relevant events are monitored via audit logs and are kept to assist in future investigations and access control monitoring. Your information gathered includes:

- User IDs.
- Dates and times for log-on and log-off.
- Terminal identity or location if possible.
- Records of successful and rejected system access attempts.
- Records of successful and rejected data and other resource access attempts.

**Risk Factors**

The result of the monitoring activities will be reviewed regularly. The frequency of the review will depend on the risks involved. Risk factors that will be considered include:

- The criticality of the application processes.
- The value, sensitivity or criticality of the information involved.
- The past experience of system infiltration and misuse.
- The extent of system interconnection (particularly public networks).

**Clock Synchronization**

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.
Mobile Computing

When you use mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, you must take special care (especially in public places) to ensure that business information is not compromised. Proper care includes physical protection, access controls, cryptographic techniques, back-ups, and virus protection.

9.1.8.1 Question 23: Your company has established a formal user registration and de-registration procedure for granting access to all multi-user information systems and services. Which of the following are not access control guidelines?
   a) You will not be granted access until authorization procedures have been completed.
   b) You will be allowed to share your userid with coworkers in your group or department.
   c) You will only have access that is consistent with your business purpose.
   d) You access will be removed immediately after you have changed jobs or left the organization.

9.1.8.2 Question 24: Which of the following is not a terminal logon guideline?
   a) You will have access to application identifiers or help messages until the log-on process has been successfully completed to prevent unnecessary system lockouts.
   b) You will be limited by the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.
   c) You will be warned by a general notice warning that the computer should only be accessed by authorized users and will be prosecuted if you are unauthorized.
   d) You will be limited in the number of unsuccessful log-on attempts allowed (three is recommended). Upon unsuccessful attempt, you will not be notified what caused the login failure.

9.1.8.3 Question 25: Which of the following is not a proper care technique that should be exercised in mobile computing?
   a) Access controls and cryptographic techniques.
   b) Physical protection and virus protection.
   c) Backups.
   d) Choosing the correct 10-10 number for long distance mobile computing.

9.1.8.4 Question 26: Which of the following is not a password guideline?
   a) You must use passwords in an automated log-on process whenever possible to keep the password from being intercepted while entering the password.
   b) You must keep passwords confidential and avoid keeping a paper record of passwords, unless this can be stored securely.
   c) You must change your password whenever there is any indication of possible system or password compromise.
   d) You password must contain at least one number, one upper case letter, and one lower case letter.
   e) Your password must have an eight character minimum length.
9.1.8.5 Question 27: You will ensure that unattended equipment has appropriate protection. Which of the following is not a guideline for unattended equipment.

a) You must power down machines when not in use to prevent any unknown vulnerability from being exposed while the system is unattended.
b) You must terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver.
c) You must log-off mainframe computers when the session is finished.
d) You must secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

9.1.9 Domain 8: Systems Development and Maintenance

Security Requirements of Systems

Security requirements will be identified and agreed prior to the development of information systems. Controls introduced at the design state are significantly cheaper to implement and maintain than those included during or after implementation.

Security in Application Systems

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical organizational assets. Such controls will be determined on the basis of security requirements and risk assessment.

Input Data Validation

Data input to application systems will be validated to ensure that it is correct and appropriate. Checks will be applied to the input of business transactions, standing data (names and addresses, credit limits, customer reference numbers) and parameter tables (sales prices, currency conversion rates, tax rates).

Areas of Risk

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks must be incorporated into systems to detect such corruption.

Message Authentication

Message authentication is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message. Message authentication will be considered for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer, specifications, contracts, proposals etc with high importance or other similar electronic data exchanges.
Output Data Validation

Data output from an application system will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Typically, systems are constructed on the premise that having undertaken appropriate validation, verification and testing the output will always be correct. This is not always the case.

Cryptographic Controls

Cryptographic systems and techniques will be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection. Your company has developed a policy on its use of cryptographic controls for protection of its information. The following will be considered:

- The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected.
- The approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys.
- Roles and responsibilities.
- The standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes).

Encryption

Encryption is a cryptographic technique that can be used to protect the confidentiality of information. It will be considered for the protection of sensitive or critical information.

Digital Signatures

Digital signatures provide a means of protecting the authenticity and integrity of electronic documents. Digital signatures can be applied to any form of document being processed electronically, e.g. they can be used to sign electronic payments, funds transfers, contracts and agreements. You must take care to protect the confidentiality of the private key. This key will be kept secret since anyone having access to this key can sign documents, e.g. payments, contracts, thereby forging the signature of the owner of that key. The two types of cryptographic techniques are:

- Secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information. This key has to be kept secret since anyone having access to it is able to decrypt all information being encrypted with that key, or to introduce unauthorized information.
- Public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret). Public key techniques can be used for encryption and to produce digital signatures.
Standards, Procedures and Methods

A key management system will be established based on an agreed set of standards, procedures and secure methods for:

- Generating keys for different cryptographic systems and different applications as well as public key certificates.
- Distributing keys to intended users, including how keys should be activated when received.
- Storing and archiving keys, including how authorized users obtain access to keys.
- Changing or updating keys including rules on when keys should be changed and how this will be done.
- Revoking and destroying as well as dealing with compromised keys.
- Recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information.
- Logging of key activities.

In order to reduce the likelihood of compromise, keys will have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time will be dependent on the circumstances under which the cryptographic control is being used and the perceived risk.

Control of Operational Software

Control will be provided for the implementation of software on operational systems. To minimize the risk of corruption of operational systems, the following controls will be implemented:

- You must only perform updates upon management authorization.
- If possible, you must only hold executable code on operational systems.
- You must not implement untested code in operational systems.
- You must maintain an audit log of all updates to operational program libraries.
- You must retain previous versions of software as a contingency measure.
- You must take into account the impact to security with any operational change.
- You must only make changes to operational systems if you have appropriate authorization.

Protection of System Test Data

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data. You must avoid the use of operational databases containing personal information. You must apply the following controls to protect operational data, when used for testing purposes:

- You must use the same procedures for operational systems.
You must receive a separate authorization every time operational information is copied to a test application system.

- You must erase operational information from a test application system immediately after the testing is complete.
- You must log the copying and use of operational information to provide an audit trail.

**Access Control to Program Source Library**

In order to reduce the potential for corruption of computer programs, you must maintain strict control over access to program source libraries to prevent the introduction of compromised code into operation systems. There are strict change control procedures over the implementation of changes to which you must adhere. They ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. This includes such practices as separating development from operations, storing code and listings in a secure environment, logging access to code, obtaining authorization for changes, etc.

**Restrictions on Changes to Software Packages**

You are encouraged to use vendor-supplied software without modifications. It is generally riskier and less secure to introduce modified vendor code. You must gain authorization before making modifications taking into account vendor consent, software integrity, organizational impact, the security gain of changes, etc. You must document and test all changes to original software and consider the use of upgrades as a solution.

**Covert Channels and Trojan Code**

A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream. Trojan code is designed to affect a system in a way that is not authorized and not readily noticed and not required by the recipient or user of the program.

Where covert channels or Trojan code are a concern, the following will be considered:

- Buying programs only from a reputable source.
- Buying programs in source code so the code may be verified.
- Using evaluated products.
- Inspecting all source code before operational use.
- Controlling access to, and modification of, code once installed.
- Use staff of proven trust to work on key systems.

Apply the same scrutiny for code from outsourced developers.
9.1.9.1 Question 28: Why is security considered during system development and maintenance?
   a) It meets all federal safety standards for information security.
   b) It is too late to introduce controls during or after implementation.
   c) Controls introduced at the design state are significantly cheaper to implement and maintain than those included during or after implementation.

9.1.9.2 Question 29: To minimize the risk of corruption of operational systems, guidelines for updating systems are put in place. Which of the following is not such a guideline?
   a) You must not implement untested code in operational systems.
   b) You must retain previous versions of software as a contingency measure.
   c) You must store source and executable code on operational systems such that in the event that a corruption is introduced, it can be quickly corrected.
   d) You must take into account the impact to security with any operational change.

9.1.10 Domain 9: Business Continuity Management

Aspects of Business Continuity Management

A business continuity management process will be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. The process takes into account the risks of these events including their likelihood and impact, possible benefit of insurance, business continuity, etc.

Business Continuity and Impact Analysis

Business continuity will begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This will be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). Both of these activities will be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes, and is not limited to the information processing facilities.

Business Continuity Planning Framework

A single framework of business continuity plans will be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance. Each business continuity plan will specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, established emergency procedures, e.g. evacuation plans or any existing fallback arrangements should be amended as appropriate.

A business continuity planning framework will include the following:
Security Awareness Training Owner’s Manual

- The conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated.

- Emergency procedures that describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities, e.g. police, fire service and local government.

- Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales.

- Resumption procedures which describe the actions to be taken to return to normal business operations.

- A maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan.

- Awareness and education activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective.

- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

Testing, Maintaining and Re-Assessing the Plans

Business continuity plans will be tested regularly to ensure that they are up to date and effective. Such tests will also ensure that all members of the recovery team and other relevant staff are aware of the plans.

Business continuity plans will be maintained by regular reviews and updates to ensure their continuing effectiveness. Examples of situations that might necessitate updating plans include the acquisition of new equipment, or upgrading of operational systems and changes in personnel, customers, contractors, etc.

9.1.10.1 Question 30: A business continuity management process reduces the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

   a) True
   b) False

9.1.10.2 Question 31: Business continuity plans will be tested regularly to ensure that they are up to date and effective. Such tests will also ensure that all members of the recovery team and other relevant staff are aware of the plans.

   a) True
   b) False

9.1.11 Domain 10: Compliance

Compliance with Legal Requirements
The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements will be sought from the organization’s legal advisers, or suitably qualified legal practitioners.

Copyright

Appropriate procedures will be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trademarks.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization, or that is licensed or provided by the developer to the organization, can be used. You must verify if you have appropriate licenses to use material which may be copyrighted.

Safeguarding of company Records

All records of the company must be protected from premature loss, destruction and falsification. You must take precaution in handling company records to prevent corruption of records or violation of legal statutes.

Records will be categorized into record types, e.g. accounting records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys associated with encrypted archives or digital signatures, will be kept securely and made available to authorized persons when needed.

To ensure information security and records management compliance, your company observes the following steps:

- Guidelines provided from and through the Records and Information Management Office on the retention, storage, handling and disposition of records and information will be observed by all departments.
- Retention schedules identifying all record types and the period of time for which they should be retained will be created, maintained, and observed.
- An inventory of sources of key information will be maintained.
- Appropriate controls will be implemented to protect essential records and information from loss, destruction and falsification.

Data Protection and Privacy of Personal Information

As a data owner, it is your responsibility to inform the Computer Information Security Officer about any proposals to keep personal information in a structured file and to ensure awareness of the data protection principles defined in the relevant legislation.
Prevention of Misuse of Information Processing Facilities

The information processing facilities of an organization are provided for business purposes. If you use these facilities for non-business or unauthorized purposes, without management approval, you will be reprimanded and possibly terminated or prosecuted for improper use of the facilities.

Rules for Evidence

It is necessary to have adequate evidence to support an action against a person or organization. Whenever this action is an internal disciplinary matter the evidence necessary will be described by internal procedures.

Where the action involves the law, either civil or criminal, the evidence presented will conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. In general, these rules cover:

- Admissibility of evidence: whether or not the evidence can be used in court.
- Weight of evidence: the quality and completeness of the evidence.
- Adequate evidence that controls have operated correctly and consistently (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed by the system.

Quality and Completeness of Evidence

To achieve quality and completeness of the evidence, a strong evidence trail is needed. In general, such a strong trail can be established under the following conditions.

- For paper documents: the original is kept securely and it is recorded who found it, where it was found, when it was found and who witnessed the discovery. Any investigation will ensure that originals are not tampered with.
- For information on computer media: copies of any removable media, information on hard disks or in memory will be taken to ensure availability. The log of all actions during the copying process will be kept and the process will be witnessed. One copy of the media and the log will be kept securely.

A lawyer or the police will be involved early in any contemplated legal action and provide advice on the evidence required.

Reviews of Security Policy and Technical Compliance

The security of information systems will be regularly reviewed against the appropriate security policies and the technical platforms and information systems will be audited for compliance with security implementation standards.
Managers will ensure that all security procedures within their area of responsibility are carried out correctly. In addition, you will be considered for regular review to ensure compliance with security policies and standards.

**Technical Compliance Checking**

Information systems will be regularly checked for compliance with security implementation standards. This extends to operational systems (hardware and software), testing systems, etc. Any technical compliance check will only be carried out by, or under the supervision of, competent, authorized persons and caution will be exercised not to disrupt the security of the systems.

**System Audit Controls**

Audit requirements and activities involving checks on operational systems will be carefully planned and agreed to minimize the risk of disruptions to business processes. Audits must be approved by the appropriate management with all procedures and access will be logged.

**9.1.11.1 Question 32: How does compliance effect information systems?**

a) The design, operation, use and management of information systems must conform to the hardware specifications.

b) The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.

c) The design, operation, use and management of information systems must meet industry standards for IT development.

d) It makes them feel good.

**9.1.11.2 Question 33: To ensure information security and records management compliance, the company observes record safeguards. Which of the following is not a safeguard?**

a) An inventory of sources of key information will be maintained.

b) Copies will be kept of all records by administrative assistants as an extra point of retention.

c) Appropriate controls will be implemented to protect essential records and information from loss, destruction and falsification.

d) Retention schedules identifying all record types and the period of time for which they should be retained will be created, maintained, and observed.

**10 Exam Answers**

Below are the exam answers as initially released with the security awareness training and exam:

1. 3 (d)
2. 0 (a)
3. 1 (b)
11 Support

Secure Commerce Systems stands behind all of its products and services and are committed to our customers. If you need support for the security awareness training and exam, please contact us via updated contact information at http://www.securecommercesystems.com/contact.html. You can also choose to open up a trouble ticket by using the Secure Commerce Systems trouble ticket system at http://www.securecommercesystems.com/GT Trouble Ticket System.html.