APPENDIX H
SECURITY POLICY RELATED DOCUMENTS

William Stallings

Supplement to
Computer Security, Third Edition
Pearson 2014
http://williamstallings.com/ComputerSecurity

H.1 A COMPANY'S PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

To give the reader a feel for how organizations deal with physical security, we provide a real-world example of a physical security policy. The company is an EU-based engineering consulting firm that specializes in the provision of planning, design, and management services for infrastructure development worldwide. With interests in transportation, water, maritime, and property, the company is undertaking commissions in over 70 countries from a network of more than 70 offices.

The following is extracted from the company's security standards document.[1] For our purposes, we have changed the name of the company to *Company* wherever it appears in the document. The company's physical security policy relies heavily on ISO 27002 (*Code of Practice for Information Security Management*).

5. Physical and Environmental security

5.1. Secure Areas

5.1.1. ***Physical Security Perimeter -*** Company shall use security perimeters to protect all non-public areas, commensurate with the value of the assets therein. Business critical information processing facilities located in unattended buildings shall also be alarmed to a permanently manned remote alarm monitoring station.

5.1.2. ***Physical Entry Controls -*** Secure areas shall be segregated and protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Similar controls are also required where the building is shared with, or accessed by, non-Company staff and organisations not acting on behalf of Company.

5.1.3. ***Securing Offices, Rooms and Facilities -*** Secure areas shall be created in order to protect office, rooms and facilities with special security requirements.

5.1.4. ***Working in Secure Areas -*** Additional controls and guidelines for working in secure areas shall be used to enhance the security provided by the physical control protecting the secure areas.

> *Employees of Company should be aware that additional controls and guidelines for working in secure areas to enhance the security provided by the physical control protecting the secure areas might be in force. For further clarification they should contact their Line Manager.*

---

[1] The entire document is provided in the Premium content section of this book's Web site (ComputerSecurityPolicy.pdf).

5.1.5. ***Isolated Access Points -*** Isolated access points, additional to building main entrances (e.g. Delivery and Loading areas) shall be controlled and, if possible, isolated from secure areas to avoid unauthorised access.

5.1.6. ***Sign Posting Of Computer Installations*** - Business critical computer installations sited within a building must not be identified by the use of descriptive sign posts or other displays. Where such sign posts or other displays are used they must be worded in such a way so as not to highlight the business critical nature of the activity taking place within the building.

5.2. Equipment Security

5.2.1. ***Equipment Sitting and Protection*** - Equipment shall be sited or protected to reduce the risk from environmental threats and hazards, and opportunity for unauthorised access.

5.2.2. ***Power Supply*** - The equipment shall be protected from power failure and other electrical anomalies.

5.2.3. ***Cabling Security*** - Power and telecommunication cabling carrying data or supporting information services shall be protected from interception or damage commensurate with the business criticality of the operations they serve.

5.2.4. ***Equipment Maintenance*** - Equipment shall be maintained in accordance with manufacturer's instruction and/or documented procedures to ensure its continued availability and integrity.

5.2.5. ***Security of Equipment off-premises*** - Security procedures and controls shall be used to secure equipment used outside any Company's premises

Employees are to note that there should be security procedures and controls to secure equipment used outside any Company premises. Advice on these procedures can be sought from the Group Security Manager.

5.2.6. ***Secure Disposal or Re-use of Equipment*** - Information shall be erased from equipment prior to disposal or reuse.

For further guidance contact the Group Security Manager.

5.2.7. ***Security of the Access Network*** - Company shall implement access control measures, determined by a risk assessment, to ensure that only authorised people have access to the Access Network (including: cabinets, cabling, nodes etc.).

5.2.8. ***Security of PCs*** - Every Company owned PC must have an owner who is responsible for its general management and control. Users of PCs are personally responsible for the physical and logical security of any PC they use. Users of Company PCs are personally responsible for the physical and logical security of any PC they use,

as defined within the Staff Handbook.

5.2.9. ***Removal of "Captured Data"*** - Where any device (software or hardware based) has been introduced to the network that captures data for analytical purposes, all data must be wiped off of this device prior to removal from the Company Site. The removal of this data from site for analysis can only be approved by the MIS Technology Manager.

5.3. General Controls

5.3.1. Security Controls - Security Settings are to be utilised and configurations must be controlled

No security settings or software on Company systems are to be changed without authorisation from MIS Support

5.3.2. ***Clear Screen Policy*** - Company shall have and implement clear-screen policy in order to reduce the risks of unauthorised access, loss of, and damage to information.

This will be implemented when all Users of the Company system have Windows XP operating system.

When the User has the Windows XP system they are to carry out the following:

- *Select the Settings tab within the START area on the desktop screen.*
- *Select Control Panel.*
- *Select the icon called DISPLAY.*
- *Select the Screensaver Tab.*
- *Set a Screen saver.*
- *Set the time for 15 Mins.*
- *Tick the Password Protect box; remember this is the same password that you utilise to log on to the system.*

Staff are to lock their screens using the Ctrl-Alt-Del when they leave their desk

5.3.3. **Clear Desk Policy –** Staff shall ensure that they operate a Clear Desk Policy

Each member of staff is asked to take personal and active responsibility for maintaining a "clear desk" policy whereby files and papers are filed or otherwise cleared away before leaving the office at the end of each day

5.3.4. ***Removal of Property*** - Equipment, information or software belonging to the organisation shall not be removed without authorisation.

Equipment, information or software belonging to Company shall not be removed without authorisation from the Project Manager or Line Manager and the MIS Support.

5.3.5. ***People Identification*** - All Company staff must have visible the appropriate identification whenever they are in Company premises.

5.3.6. **Visitors** - All Company premises will have a process for dealing with visitors. All Visitors must be sponsored and wear the appropriate identification whenever they are in Company premises.

5.3.7. ***Legal Right of Entry*** - Entry must be permitted to official bodies when entry is demanded on production of a court order or when the person has other legal rights. Advice must be sought from management or the Group Security Manager as a matter of urgency.

H.2 SECURITY POLICY STANDARD OF GOOD PRACTICE

This specifications is from *The Standard of Good Practice for Information Security* [ISF11].

Principle: A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems.

Objective: To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

1. There should be a documented information security policy, ratified at top level, that applies across the enterprise. There should be an individual (or a group of individuals) responsible for maintaining the policy.

2. The information security policy should define information security, associated responsibilities and the information security principles to be followed by all staff.

3. The information security policy should require:
a) critical information and systems to be subjected to a risk analysis on a regular basis
b) that an 'owner' - typically the person in charge of a particular business application, computer installation or network - is assigned for all critical information and systems
c) that information and systems are classified in a way that indicates their criticality to the enterprise
d) that staff are made aware of information security
e) compliance with software licenses and with legal, regulatory and contractual obligations
f) breaches of the security policy and suspected security weaknesses to be reported
g) information to be protected in terms of its requirements for confidentiality, integrity and availability.

4. A high level policy (e.g. the information security policy) should prohibit:
a) using the enterprise's information and systems without authorization or for purposes that are not work-related
b) making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
c) making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
d) downloading illegal material (e.g. with obscene or discriminatory content)
e) the movement of information or equipment off-site without authorization

f) unauthorized use of information, facilities or equipment
g) unauthorized copying of information/software
h) compromising passwords (e.g. by writing them down or disclosing them to others)
i) using personally identifiable information for business purposes unless explicitly authorized
j) discussing business information in public places
k) tampering with evidence in the case of an incident.

5. A high level policy (e.g. the information security policy) should state that users should:
a) lock away sensitive media or documentation when not in use (i.e. complying with a 'clear desk' policy)
b) log-off systems in use when leaving a terminal/workstation unattended (e.g. during a meeting, lunch break or overnight).

6. The information security policy should be:
a) communicated to all staff and external parties with access to the enterprise's information or systems
b) reviewed regularly according to a defined review process
c) revised to take account of changing circumstances.

7. The information security policy should state that disciplinary actions may be taken against individuals who violate its provisions.

H.3 SECURITY AWARENESS STANDARD OF GOOD PRACTICE

These specifications are from *The Standard of Good Practice for Information Security* [ISF05].

Security Management

Focus: Security management at the enterprise level

Principle: Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the enterprise.

Objective: To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.

1. Specific activities should be performed to promote security awareness (the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities – and act accordingly) across the enterprise. These activities should be:
a) endorsed by top management
b) the responsibility of a particular individual, organisational unit, working group or committee
c) supported by a documented set of objectives
d) delivered as part of an on-going security awareness programme
e) subject to project management disciplines
f) kept up-to-date with current practices and requirements
g) based on the results of a risk assessment
h) aimed at reducing the frequency and magnitude of incidents
i) measurable.

2. Security awareness should be promoted:
a) to top management, business managers/users, IT staff and external personnel
b) by providing information security education/training, such as via computer-based training (CBT)
c) by supplying specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.

3. Staff should be provided with guidance to help them understand:
a) the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)

b) the importance of complying with information security policy and applying associated standards/procedures
c) their personal responsibilities for information security.

4. The effectiveness of security awareness should be monitored by measuring:
a) the level of security awareness in staff and reviewing it periodically
b) the effectiveness of security awareness activities, for example by monitoring the frequency and magnitude of incidents experienced.

5. Security-positive behaviour should be encouraged by:
a) making attendance at security awareness training compulsory
b) publicising security successes and failures throughout the organisation
c) linking security to personal performance objectives/appraisals.

Critical Business Applications

Focus: A business application that is critical to the success of the enterprise

Principle: Users of the application should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure users of the application apply security controls and prevent the security of information used in the application from being compromised.

1. Users of the application should be covered by an information security policy. They should be aware of the policy and comply with it.

2. Users of the application should:
a) take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities – and act accordingly)
b) be provided with information security education/training, such as via computer-based training (CBT)
c) be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.

3. Users of the application should be made aware of:
a) the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the application
c) the importance of complying with information security policies and applying associated standards/procedures
d) their personal responsibilities for information security.

4. Users of the application should be made aware that they are prohibited from:
a) using information or systems without authorisation

b) using the application for purposes that are not work-related
c) making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
d) making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
e) downloading illegal material (e.g. with obscene or discriminatory content)
f) using unauthorised application components (e.g. installing unauthorised third party software or modems)
g) unauthorised copying of information or software
h) disclosing confidential information (e.g. customer records, product designs and pricing policies)
i) compromising passwords (e.g. by writing them down or disclosing them to others)
j) using personally identifiable information for business purposes unless explicitly authorised
k) tampering with evidence in the case of incidents that may require forensic investigation.

5. Users of the application should be warned of the dangers of being overheard when discussing business information either over the telephone or in public places (e.g. train carriages, airport lounges or bars).

Computer Installations

Focus: A computer installation that supports one or more business applications

Principle: Staff running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure that staff running the installation apply security controls and prevent the security of information used in the computer installation from being compromised.

1. There should be an information security policy that applies to the computer installation. Staff employed in the computer installation should be aware of the policy and comply with it.

2. Staff employed in the computer installation should:
a) take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities – and act accordingly)
b) be provided with information security education/training, such as via computer-based training (CBT)

c) be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.

3. Staff employed in the computer installation should be made aware of:
a) the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the installation
c) the importance of complying with information security policies and applying associated standards/procedures
d) their personal responsibilities for information security.

4. Staff employed in the computer installation should be made aware that they are prohibited from:
a) using any part of the installation without authorisation or for purposes that are not work-related
b) making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
c) making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
d) downloading illegal material (e.g. with obscene or discriminatory content)
e) using unauthorised installation components (e.g. installing unauthorised third party software or modems)
f) unauthorised copying of information or software
g) disclosing confidential information (e.g. customer records, product designs or pricing policies)
h) compromising passwords (e.g. by writing them down or disclosing them to others)
i) using personally identifiable information for business purposes unless explicitly authorised
j) tampering with evidence in the case of incidents that may require forensic investigation.

Networks

Focus: A network that supports one or more business application

Principle: Network staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure network staff apply security controls and prevent the security of information transmitted across the network from being compromised.

1. There should be an information security policy that applies to the network. Network staff should be aware of the policy and comply with it.

2. Network staff should:

a) take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities – and act accordingly)
b) be provided with information security education/training, such as via computer-based training (CBT)
c) be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.

3. Network staff should be made aware of:
a) the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the network
c) the importance of complying with information security policies and applying associated standards/procedures
d) their personal responsibilities for information security.

4. Network staff should be made aware that they are prohibited from:
a) using any part of the network without authorisation or for purposes that are not work-related
b) making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
c) making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
d) downloading illegal material (e.g. with obscene or discriminatory content)
e) using unauthorised network components (e.g. installing unauthorised third party software or modems)
f) unauthorised copying of information or software
g) disclosing confidential information (e.g. network designs or IP addresses)
h) compromising passwords (e.g. by writing them down or disclosing them to others)
i) using personally identifiable information for business purposes unless explicitly authorised
j) tampering with evidence in the case of incidents that may require forensic investigation.

Systems Development

Focus: A systems development unit/department or a particular systems development project.

Principle: Systems development staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure systems development staff apply security controls and prevent the security of information used in development activities from being compromised.

1. There should be an information security policy that applies to development activities. Development staff should be aware of the policy and comply with it.

2. Development staff should:
a) take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities – and act accordingly)
b) be provided with information security education/training, such as via computer-based training (CBT)
c) be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.

3. Development staff should be made aware of:
a) the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect systems development activities
c) the importance of complying with information security policies and applying associated standards/procedures
d) their personal responsibilities for information security.

4. Development staff should be made aware that they are prohibited from:
a) using information or systems without authorisation or for purposes that are not work-related
b) making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
c) making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
d) downloading illegal material (e.g. with obscene or discriminatory content)
e) using unauthorised system components (e.g. installing unauthorised third party software or modems)
f) unauthorised copying of information or software
g) disclosing confidential information (e.g. development designs, IP addresses or details of external connections)
h) compromising passwords (e.g. writing them down or disclosing them to others)
i) using personally identifiable information for business purposes unless explicitly authorised
j) tampering with evidence in the case of incidents that may require forensic investigation.

H.4 INFORMATION PRIVACY STANDARD OF GOOD PRACTICE

This specification is from *The Standard of Good Practice for Information Security* [ISF11].

Principle: Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.

Objective: To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.

1. A high-level committee (or equivalent) should be established to be responsible for managing information privacy issues, and an individual appointed to co-ordinate information privacy activity (e.g., a Chief Privacy Officer).

2. The high-level committee (or equivalent) should be aware of:
a) the location(s) of all personally identifiable information held on individuals
b) how and when personally identifiable information is used.

3. There should be documented standards/procedures for dealing with information privacy, which should cover:
a) acceptable use of personally identifiable information
b) the rights of individuals about whom personally identifiable information is held
c) privacy assessment, awareness and compliance programs
d) legal and regulatory requirements for privacy.

4. Where personally identifiable information is stored or processed, there should be processes to ensure that it is:
a) adequate, relevant and not excessive for the purposes for which it is collected
b) accurate (i.e. recorded correctly and kept up-to-date)
c) kept confidential, processed fairly and legally, and used only for specified, explicit and legitimate purposes
d) held in a format that permits identification of individuals for no longer than is necessary
e) only provided to third parties that can demonstrate compliance with legal and regulatory requirements for handling personally identifiable information
f) retrievable in the event of a legitimate request for access.

5. Individuals about whom personally identifiable information is held (e.g. the 'data subject' according to the EU Directive on Data Protection) should:
a) have their approval sought before this information is collected, stored, processed or disclosed to third parties
b) be informed of how this information will be used, allowed to check its accuracy and able to have their records corrected or removed.

6. Personally identifiable information should be handled in accordance with relevant legislation, such as the EU Directive on Data Protection or the US Health Insurance Portability and Accounting Act (HIPAA).

7. An individual (or group) throughout the enterprise should:
a) perform a privacy assessment (e.g. to determine the level of compliance with relevant legislation and internal policies)
b) implement a privacy compliance program
c) make staff and third parties aware of the importance of information privacy.

H.5 INCIDENT HANDLING STANDARD OF GOOD PRACTICE

This specification is from *The Standard of Good Practice for Information Security* [ISF11].

Application Management

Principle: All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

1. All incidents that affect the application (including malicious attacks, abuse/misuse of systems by staff, loss of power/communications services and errors by users or computer staff) should be dealt with in accordance with an incident management process.

2. The incident management process should be documented, and cover reporting and recording of incidents, investigating and resolving incidents, reviewing patterns of incidents, and escalation processes.

3. Incidents should be:
a) reported to a single point of contact, such as a help desk, telephone hot line or individual IT specialist
b) documented, typically using an automated incident management system
c) categorised by type (e.g. malfunctions, malicious attack or internal abuse/misuse of systems)
d) prioritised according to their impact/urgency.

4. The business impact of significant incidents should be assessed by an IT specialist, the application 'owner' and an information security specialist.

5. The resolution of incidents should include:
a) investigating their root causes
b) planning corrective action to ensure security is not affected
c) restricting access when corrective actions are performed
d) documenting corrective actions taken
e) performing a review to ensure that the security of the application has not been affected by the incident or its resolution.

6. Patterns of incidents should be reviewed to identify potential security breaches and minimise the chances of similar incidents disrupting the application – or other applications – in the future.

System Operation

Principle: All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

1. All incidents that affect the installation (including third party attack, internal misuse/abuse, malfunctions, loss of power/communications services, overloads and mistakes by users or computer staff) should be dealt with in accordance with an incident management process.

2. The incident management process should be documented, and cover reporting and recording of incidents, investigating and resolving incidents, reviewing patterns of incidents, and escalation processes.

3. Incidents should be:
a) reported to a single point of contact, such as a help desk, telephone hot line or individual IT specialist
b) documented, typically using an automated incident management system
c) categorised by type (e.g. malfunctions, malicious attack or internal abuse/misuse of systems)
d) prioritised according to their impact/urgency.

4. The business impact of significant incidents should be assessed by an IT specialist, the 'owner' of an application supported by the installation and an information security specialist.

5. The resolution of incidents should include:
a) investigating their root causes
b) planning corrective action to ensure security is not affected
c) restricting access when corrective actions are performed
d) documenting corrective actions taken
e) performing a review to ensure that the security of the installation has not been affected by the incident or its resolution.

6. Patterns of incidents should be reviewed to identify potential security breaches and minimise the chances of similar incidents disrupting the installation – or other installations – in the future.

Network Operations

Principle: All network incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective: To identify and resolve network incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

1. All incidents that affect the network (including third party attack, internal misuse/abuse, malfunctions, loss of power/communications services, overloads and mistakes by users or computer staff) should be dealt with in accordance with an incident management process.

2. The incident management process should be documented, and cover reporting and recording of incidents, investigating and resolving incidents, reviewing patterns of incidents, and escalation processes.

3. Network incidents should be:
a) reported to a single point of contact, such as a help desk, telephone hotline or individual IT specialist
b) documented, typically using an automated incident management system
c) categorised by type (e.g. malfunctions, malicious attack or internal abuse/misuse of the network)
d) prioritised according to their impact/urgency.

4. The business impact of significant network incidents should be assessed by a network specialist, the network 'owner', 'owners' of the applications supported by the network and an information security specialist.

5. The resolution of network incidents should include:
a) investigating their root causes
b) planning corrective action to ensure security is not affected
c) restricting access when corrective actions are performed
d) documenting corrective actions taken
e) performing a review to ensure that the security of the network has not been affected by the incident or its resolution.

6. Patterns of network incidents should be reviewed to identify potential security breaches and minimise the chances of similar incidents disrupting the network – or other networks – in the future.