State of Ohio IT Guideline Information Technology Business Continuity Planning	**Published By:** Statewide IT Policy Investment and Governance Division Office of Information Technology Publication Date: 03/17/2008

1.0 Purpose

This document provides state agencies guidance in the development and implementation of a comprehensive information technology ***business continuity plan*** that, in the event of a business disruption, will help enable the continuation of critical processes and the delivery of essential services at an acceptable level.

2.0 Background

Business disruptions are unplanned interruptions that may develop from a variety of sources such as natural disasters, health pandemics, technology failures or criminal acts. The impact of a disruption can be severe enough to threaten the very survival of an organization. Such disruptions cannot always be predicted or prevented, but effective planning can dramatically reduce the damage they cause. The ability for critical processes to persist despite a disruption is known as ***business continuity***.

Prior to developing a business continuity plan, two essential types of analysis need to be completed: a ***business impact analysis*** that identifies and prioritizes critical business functions, and a ***risk assessment*** that identifies ***threats*** and their probability of occurrence. By relating the results of the business impact analysis to the risk assessment, agencies can identify how likely it is that a particular threat will affect a critical system. When these steps have been completed, an effective business continuity plan can be developed that provides for the continuation of critical processes and the delivery of essential services despite disruptions.

3.0 References

3.1 Ohio IT Policy ITP-B.1, “Information Security Framework,” is the overarching security policy for state information and services. Attachment 1 illustrates the interrelationship of state technology security policies.

3.2 Ohio IT Policy ITP-B.5, “Remote Access Security,” requires state agencies to implement and operate security measures wherever a remote access capability is provided to state systems so that inherent vulnerabilities in such services may be compensated.

3.3 Ohio IT Policy ITP-B.8, “Security Education and Awareness,” requires state agencies to provide information technology security education and awareness to employees, contractors, temporary personnel and other agents of the state who use and administer state computer and telecommunications systems.

3.4 Ohio IT Policy ITP-B.11, “Data Classification,” provides a high-level data classification methodology to state agencies for the purpose of understanding and managing data and information assets with regard to their level of ***confidentiality*** and criticality.

3.5 Ohio IT Bulletin ITB-2007.02, “Data Encryption and Securing Sensitive Data,” effective July 25, 2007, outlines the requirements for the encryption of sensitive

data as well as requirements for securing portable devices and media, backups, sensitive data in transmission, and sensitive data at rest. The bulletin also outlines restrictions for sensitive data, physical security considerations, public servant acknowledgement requirements, and incident response.

3.6 Ohio Revised Code section 149.433, exempts certain types of security and infrastructure records from mandatory release or disclosure under Ohio's public records laws. The exemptions are intended to help protect critical information regarding agency security practices and vulnerabilities.

3.7 A glossary of terms found in this document is located in Section 5.0 – Definitions. The first occurrence of a defined term is in ***bold italics***.

4.0 Information Technology Business Continuity Planning

State agencies should establish an information technology business continuity plan that provides for the continuation of critical business functions that are supported by technology in the event of a disruption. The plan should also facilitate the agency's ability to resume normal information technology business operations as soon as possible. This document outlines the preparation activities and key components necessary for the development of an effective business continuity plan.

4.1 Business Continuity Plan Preparation. Prior to developing a business continuity plan, agencies should address:

4.1.1 Scope of Coverage. Agencies should define the scope of coverage of their business continuity plan and the extent to which it affects and overlaps with the plans of other agencies and stakeholders.

Agencies should consider three factors in defining the scope of coverage for their business continuity plan:

- Whether the agency business continuity plan integrates with other Ohio agency, local government, or other state and federal business continuity and emergency plans, especially where the authority of one plan may supersede another;
- Whether other stakeholders relevant to the agency's mission, including private-sector partners, warrant inclusion in the business continuity plan; and
- Whether the agency business continuity plan addresses situations that would require the activation of other local, state or federal business continuity or emergency plans.

4.1.2 Development Team. Agencies should assemble a business continuity plan development team, with representatives from all functional areas of the agency, including senior management. A plan coordinator should be assigned to oversee the development and implementation of the business continuity plan.

4.1.3 Business Impact Analysis. Agencies should conduct a business impact analysis to characterize, quantify and prioritize the agency's applications and business functions supported by technology and to identify key

personnel, vendors, hardware and software. Business impact analysis involves identifying the critical business functions within the organization and determining the impact of not performing these functions beyond the ***maximum acceptable outage***. The business impact analysis should consider a range of possible disruptions, including ***natural***, ***human*** and ***environmental threats***. The results of the business impact analysis will assist in determining the appropriate recovery strategies.

4.1.3.1 Criticality of Business Functions Supported by Technology. Agencies should identify all business functions supported by technology within their agency and determine the criticality of the function in relation to the agency's overall operations. Criticality should be measured in terms of the health and safety of the public and of state workers, financial impact, continuation of essential agency programs and services, and the legal integrity of agency operations.

4.1.3.2 Impact on Internal and External Stakeholders. Agencies should consider the impact that a business disruption would have on both internal and external stakeholders, and identify the degree of inter-dependency or interactivity that each information technology function has with other Ohio agencies, local governments, other state and federal agencies, private businesses, and the public. This analysis will assist the agency in more accurately determining the criticality of an information technology function.

4.1.3.3 Data Classification. Agencies should review data that has been classified in accordance with Ohio IT Policy ITP-B.11, "Data Classification," to identify the need for confidentiality, ***integrity*** and ***availability*** in performing agency functions and services.

4.1.3.4 Maximum Acceptable Outage or Loss. For each business function supported by technology, agencies should assign a ***recovery time objective***, which is the target time frame for the restoration of a process or service after a disruption has occurred.

In addition, agencies should determine the ***recovery point objective***, which is the latest available point in time from which data can be recovered. The recovery point objective will define parameters for an acceptable loss of data and help determine backup frequency requirements. When determining the recovery point objective, it is important to review agency record retention schedules and agency data maintenance guidelines as required in Ohio IT Policy ITP-B.11, "Data Classification," to ensure the appropriate data can be recovered.

When possible, agencies should calculate the cost of downtime and define the impact of loss of data for each business function supported by technology to help illustrate the overall impact of the recovery time objective and the recovery point objective decisions.

4.1.3.5 Business Impact Analysis Results. The outcome of the business impact analysis should be an identification of the critical business processes and their associated recovery time objectives, recovery point objectives, software, hardware, essential records, and critical resource, equipment and vendor dependencies. All mission critical systems and functions should be identified and clearly recorded as a result of this exercise. The business impact analysis should also identify interdependencies of internal and external processes, personnel requirements and known work-arounds.

4.1.3.6 Business Impact Analysis Review. The business impact analysis should be revisited as part of the overall business continuity plan update process to ensure that it is still an accurate reflection of the agency's requirements.

4.1.4 Risk Assessment. State agencies should conduct a risk assessment involving threat identification, ***vulnerability*** and control analysis to identify the most probable threats to an agency.

4.1.4.1 Threat Identification. Agencies should identify possible threats with the potential to cause harm to an information technology process or service: natural, human, or environmental.

4.1.4.2 Vulnerability Analysis. When the threats have been identified, agencies should identify and analyze the vulnerabilities that exist within their environment that could be exploited by the potential threat.

4.1.4.3 Control Analysis. Agencies should identify and analyze the controls that minimize threats or mitigate vulnerabilities. Controls include protection devices, safeguards, and procedures that are in place to reduce the effects of threats and vulnerabilities. Agencies should consider the nature of their vulnerabilities and the existence and effectiveness of current controls.

4.1.4.4 Probability Determination. For each threat identified, agencies should reference the results of the vulnerability and control analysis to estimate the likelihood of the threat occurring.

4.1.4.5 Acceptable Level of Risk. Risk cannot always be avoided; therefore, agencies should determine the level of acceptable risk for each business function supported by technology. Agencies should use the outcome of the business impact analysis to help form acceptable risk decisions. Risks may either be eliminated, mitigated, shared with one or more third parties, or accepted.

4.1.4.6 Risk Assessment Review. The risk assessment should be revisited as part of the overall business continuity plan update process to ensure that it is still an accurate reflection of the agency's risk environment.

4.1.5 Approval of Business Impact Analysis and Risk Assessment Results by Management. The final results of the business impact analysis and the risk assessment should have written approval from agency senior management before the actual plan development phase begins.

4.2 Business Continuity Plan Development. Agencies should use the results of the business impact analysis and risk assessment to develop and implement an information technology business continuity plan that will help enable the continuation of critical information technology processes and delivery of essential services at an acceptable level in the event of a disruption. The plan should also address the recovery of agency information technology facilities and capabilities if those processes or services fail. At a minimum, the agency's business continuity plan should include the following components:

4.2.1 Business Disruption Scenarios. Agencies should ensure that preparations have been made to manage a disruption in service, whether mild or severe, and resume normal operations as soon as possible. Agencies should develop a plan that anticipates a variety of disaster scenarios. The plan should incorporate protections that are common to as many scenarios as possible.

4.2.2 Plan Activation Procedures. Agencies should clearly define the events that will trigger or invoke the plan for each disruption scenario identified. As part of this process, the agency should define specific escalation and communication procedures, determine procedures for post-activation analysis, and apply lessons learned.

4.2.2.1 Escalation Level Criteria. Agencies should develop an escalation process for response based on the degree of disruption and other factors identified in the business impact analysis and risk assessment, such as the criticality of the affected function and the impact on overall operations.

4.2.3 Recovery Strategies. Agencies should develop recovery strategies to ensure that, in the event of a disruption, critical information technology functions, as identified by the business impact analysis, can still be performed. Analyzing the operational and economic impact of the disruption on the agency is an important part of defining the recovery strategy. In addition, the defined recovery time objective and recovery point objective will assist in determining the appropriate recovery strategy.

4.2.3.1 Recovery Schedule. Agencies should define a recovery schedule that clearly prioritizes the order in which critical services should resume.

4.2.3.2 People. Agencies should develop a personnel strategy to maintain critical information technology functions, including instances where full, on-site staff availability is not possible. Agencies should also consider personnel requirements when considering alternate worksites. These sites would need to accommodate the personnel required to maintain critical functions.

A clear chain of command should be defined for each disruption scenario. Personnel should be made aware of their recovery responsibilities and roles by management, including whether they are expected to ***telework***. Recovery roles should be rehearsed to the extent necessary.

Agencies should create and distribute a contact list to appropriate agency personnel consisting of names, addresses and telephone numbers of all personnel who may be required for recovery procedures.

4.2.3.3 Data. Agencies should backup and restore data based on the results of the business impact analysis.

Agencies should create and maintain timely, secure data backup files that are routinely verified for data ***integrity***. Backups should be securely maintained in a location with security at least as good as the security of the systems that generated the backup media.

Agencies should ensure that the procedures for accessing, processing and storing data remotely are defined in accordance with data risk. For sensitive data, agencies should address the requirements found in Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data."

Data recovery strategies should address the retrieval of encrypted sensitive information by authorized personnel. Encryption key management procedures should be implemented that provide for the appropriate level of confidentiality and integrity while still ensuring data access and availability by necessary personnel.

4.2.3.4 Software. Agencies should maintain verified copies of all critical system and application software, whether vendor supplied or developed in-house, and ensure that the system and application software versions and security-related patches are current. Agencies should also maintain documentation detailing any customizations affecting desktop environments or phone systems. Additional information that should be kept on file as appropriate includes:

- Date purchased
- Purchase Order number
- Contract number
- Number and types of licenses
- Manufacturer
- Maintenance / upgrade information
- Vendor information
- Vendor site logins and passwords
- In-house support contact information
- Location of original media and updates
- Information for special passwords, key codes, dongle keys, etc.

- Assets to which the software is distributed

This information should be kept in a secure off-site location along with any copies of software documentation.

4.2.3.5 Equipment. Agencies should maintain a complete, up-to-date inventory of all critical information technology equipment. At a minimum, the inventory should include:

- Date purchased
- Location
- Purchase Order number
- Model numbers
- Serial numbers
- Sales Representative information (including name, phone number, e-mail)
- Contract information
- In-house support contact information
- Add-ons or updates to the equipment
- Maintenance agreement and number
- Account information
- Vendor information

For some equipment, redundant configurations can facilitate the recovery of information technology functions while preserving evidence of a compromised information technology asset. Based on the business impact analysis and risk assessment, agencies should assess the value and need for maintaining redundant system configuration capabilities. Agencies should ensure that uninterruptible power supplies or backup generators are in place where applicable. Mission critical systems should have redundant configurations.

4.2.3.6 Communications Systems. Agencies should assess their existing communications systems and identify controls that could prevent interruption of primary communication channels. Agencies should also ensure that plans are in place for when preventative controls fail. Agencies should implement alternative forms of communication that are consistent with the findings of their business impact analysis and risk assessment. For mission critical systems, agencies should consider the need for redundant communications links, network service providers, network connecting devices and Internet service providers.

4.2.3.7 Communication Chain Strategy. Agencies should establish a communication chain strategy to use with their own employees, other agencies, citizens, and the press. This strategy should include the following elements:

- multiple, redundant forms of communications in case one or more forms should fail;
- a procedure to monitor information sources; and
- a method to disseminate important information that may aid outside parties.

Information Web sites may be used to coordinate remote employees and to convey information to the public or other agencies. Web sites established for this purpose should be located on servers in a secure facility separate from the primary work site and should conform to all state of Ohio information technology policies.

4.2.3.8 Supplies. Agencies should identify the supplies necessary for the continuation of business and determine what surplus quantities to have on hand, either on-site or off-site. A record should be maintained of the quantities, the location, and how to access the supplies, along with relevant vendor information.

4.2.3.9 Alternative Worksite. Agencies should determine their need for alternate work locations, relying on the outcomes of the business impact analysis and risk assessment for guidance. If an alternate site is necessary, it should be far enough away not to be affected by a disaster at the main site, but close enough to avoid prohibitive transportation or telecommunications costs. Alternative work site strategies may include the use of ***hot sites***, ***cold sites***, sites shared with other agencies, and telework.

4.2.3.10 Remote Access. Agencies should develop a plan to access information systems remotely in case the primary work site is not physically accessible. Agencies should develop an inventory of remote access methods and should include a method to provide bandwidth capacity and technical support for those employees who do not typically use remote access. Remote access capabilities should adhere to the security requirements outlined in Ohio IT Policy ITP-B.5, “Remote Access Security.”

4.2.3.11 Transportation. Events that disrupt the transportation of people or supplies might have a serious effect on the ability to continue to provide critical information technology functions and services. For this reason, agencies should identify alternate forms of transportation. Alternate forms of transportation may be essential if an alternate site is being used to continue critical operations.

4.2.3.12 Documentation. Agencies should store backup documentation off-site. A complete set of all pertinent documentation, such as computer operations manuals, user manuals and program maintenance manuals, should be stored in a secure off-site facility. Copies of the business continuity plan, including equipment inventories and alternate site agreements, should be stored in a secure location that is sufficiently removed from the main facility so as not to be subject to the same hazards.

Agencies should identify those backup personnel who will have access to this site and the documentation.

4.2.3.13 Procurement Procedures. To ensure that critical resources can be acquired in the event of a disruption, agencies should establish procurement procedures for each disruption scenario. Agencies should ensure that designated personnel are assigned sufficient procurement authority to provide resources necessary to continue operations during a disruption. In addition, agencies should authorize alternate agency personnel as procurement contacts to help ensure coverage in the event of a disruption.

4.2.4 Compliance Review. Agencies should conduct a compliance review of their business continuity plan with relevant staff (ie. IT, policy, communications, and legal personnel). The compliance review should determine if the agency's plan:

- complies with overall agency and state policies; and
- conforms to federal, state and local laws.

As part of the compliance review, agencies should identify potential liability issues if the agency is unable to comply with regulations in the event of a disaster.

4.2.5 Review and Approval by Management. The final business continuity plan should be reviewed and approved in writing by senior agency management.

4.3 Business Continuity Plan Distribution. Agencies should ensure business continuity plans are properly secured and distributed.

4.3.1 Business Continuity Plan Copies Stored in an Off-Site Location. Agencies should maintain copies of the agency business continuity plan and any other related critical documents and materials at a predetermined, secure off-site location. Designated personnel on the contact list should be given location and access information.

4.3.2 Coordination with Public Authorities. Agencies should ensure that, where appropriate, the existence and content of the agency business continuity plan is conveyed to other Ohio agencies, local government, or other state and federal agencies.

4.4 Business Continuity Plan Testing and Maintenance. Agencies should test their business continuity plan at least twice a year. At a minimum, one of the tests should be for the most likely scenario with tests for less likely scenarios conducted as deemed necessary. The type and extent of testing will depend on the criticality of the business function supported by technology and the complexity of its processes and components.

4.4.1 Retesting After Major Changes or Improvements. Agencies should ensure that any major changes or improvements in their processes or infrastructure are tested during the next regularly scheduled testing exercise. In the short term, agencies may want to consider conducting ***tabletop exercises*** to test the effect of major changes or improvements

on the business continuity plan. Such changes may include, but are not limited to:

- Enabling statutes or regulations
- Physical facility
- Computer hardware/software
- Telecommunications hardware/software
- Networks
- Application systems
- Organization
- Budget

4.4.2 Evaluation of Test Results. Agencies should evaluate test results to determine if the business continuity plan requires further modification for effectiveness.

4.4.2.1 Incorporation of Lessons Learned. Agencies should capture and disseminate lessons learned to reduce the possibility of similar disruptions, thereby enhancing the overall business continuity plan.

4.4.2.2 Results Kept on File and Available for Review. Results of the testing exercise should be kept on file and made available for review by authorized personnel.

4.4.2.3 Modifications Approved by Management. Any modifications made to the business continuity plan as a result of the test should have written approval from senior agency management.

4.4.3 Updated Plan Distributed to Business Continuity Team. A new copy of the business continuity plan should be distributed as appropriate and off-site copies should be replaced after each plan update.

4.5 Functional Outsourcing. Agencies should establish strong controls in information technology contracts that involve outsourcing a portion of their business or information technology functions or business continuity services. Agencies should consider whether the risks associated with maintenance of agency data preclude use of a contractor for outsourced functions.

4.5.1 Contractor Security Assessment. Agencies should ascertain that the contractor is capable of securing data in accordance with its assigned data classification label. Liability for the loss or inappropriate usage of data should be carefully defined in the service contract.

4.5.2 Contractor Financial Stability Assessment. Agencies should assess the financial stability of the contractor to determine if the contractor is stable enough financially to perform agency services for an extended period of time, especially during a prolonged emergency.

4.5.3 Contractor Business Continuity Competency Assessment. Agencies should assess whether contractors have the following business continuity controls in place:

- a business continuity plan based on business impact analysis and risk assessment;
- a testing plan for the business continuity plan that is exercised regularly;
- a statement of recovery along with particular recovery point objectives; and
- assurances that notification for service outages will be given.

4.6 Employee Education and Awareness. Agencies should establish business continuity education and awareness efforts in accordance with Ohio IT Policy ITP-B.8, "Security Education and Awareness." At a minimum, agencies should address the following:

4.6.1 Convey to all employees the rationale and importance of a business continuity plan.

4.6.2 Review the business impact analysis and risk assessment concepts and define their importance in the overall business continuity plan development process.

4.6.3 Communicate clearly to all employees what the expectations are of them should various types of disruptions occur. Ensure that every employee understands his or her role and responsibilities in the event of a disruption.

4.6.4 Identify for all employees how pertinent information will be communicated to them should various types of disruptions occur.

5.0 Definitions

5.1 Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.

5.2 Business Continuity. The ability to continue critical business processes at an acceptable level despite a disruption of business functions and services supported by technology.

5.3 Business Continuity Plan. A collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of a business disruption.

5.4 Business Impact Analysis. An information-gathering exercise used to characterize, quantify and prioritize the agency's applications and business functions supported by technology and to identify the critical business functions within an organization. The business impact analysis also assists in defining how long a function or resource can be unavailable before the impact to the organization becomes too great. The business impact analysis combined with the risk assessment will serve as the foundation for developing a business continuation strategy.

5.5 Cold Site. A facility that contains the infrastructure necessary to recover critical business functions or information systems, except for hardware and telecommunications equipment.

5.6 Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas where confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.

5.7 Environmental Threats. Events such as a long-term power failure, pollution or liquid leakage.

5.8 Hot Site. A facility that holds the infrastructure, telecommunications and hardware equipment necessary to recover critical business functions or information systems.

5.9 Human Threats. Events either intentionally or unintentionally caused by human beings, such as terrorism, pandemics, and malicious code.

5.10 Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because businesses, citizens and governments depend upon the accuracy of data in state databases, agencies must ensure that data is protected from improper change. Information systems that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.

5.11 Maximum Acceptable Outage. The maximum period of time that a given resource or function can be unavailable before the agency will sustain unacceptable consequences, such as financial loss or loss of public trust.

5.12 Natural Threats. Events such as floods, earthquakes, tornadoes and electrical storms.

5.13 Recovery Point Objective. This describes the latest available point in time from which data can be restored to be acceptable to the owner(s) of the processes supported by that data. The recovery point objective is established based on tolerance for loss of data and helps determine backup frequency requirements.

5.14 Recovery Time Objective. The target time frame for the restoration of a process or service after a disruption has occurred.

5.15 Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security. See Ohio IT Policy ITP-B.1, “Information Security Framework,” for assessment guidelines.

5.16 Tabletop Exercise. A tabletop exercise is a method of testing the business continuity plan that does not have a significant impact on daily operations. The

business continuity team reviews and discusses the actions they would take to specific disruption scenarios as outlined in their plans, but they do not actually perform any of these actions. The exercise can be conducted with a single team, or multiple teams as appropriate.

5.17 Telework. The practice of working from home via computer or other telecommunications. Synonymous with "telecommute."

5.18 Threat. An event with the potential to cause harm to an information technology process or service. A threat can be natural, human or environmental.

5.19 Vulnerability. A flaw or weakness in system security procedures, design, implementation, or internal controls of business functions supported by technology, processes or facilities which may promote or contribute to a disruption.

6.0 Related Resources

Document Name
National Institute of Standards and Technology's "Risk Management Guide for Information Technology Systems, Special Publication 800-30." http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
National Institute of Standards and Technology's "Contingency Planning Guide for Information Technology Systems." http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.
State of Ohio Enhanced Mitigation Plan. http://www.ema.ohio.gov/mitigation_plan/mitigation_plan.asp.
Ready.gov. Sample Emergency Plan. http://www.ready.gov/business/_downloads/sampleplan.pdf
USA.gov. Disasters and Emergencies: Resources for State and Local Employees. http://www.usa.gov/Government/State_Local/Disasters.shtml.

7.0 Inquiries

For questions regarding business continuity, please contact:

Risk Management Services
Ohio Office of Information Technology
1320 Arthur E. Adams Drive
Columbus, Ohio 43221

Telephone: 614-995-7632
Facsimile: 614-644-2133
E-mail: RiskManagementServices@OIT.Ohio.Gov

Direct inquiries about this document to:

Statewide IT Policy
Investment and Governance Division
Ohio Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

Telephone: 614-644-9352
Facsimile: 614-644-9152
E-mail: State.ITPolicy.Manager@oit.ohio.gov

Ohio IT Policy can be found on the Internet at: www.ohio.gov/itp.

8.0 Attachments

8.1 Attachment 1 – Interrelationship of the Information Security Framework Policy and Sub-policies. A cross-reference table showing the relationship between the primary framework policy and the sub-policies is provided and may be helpful to agencies as they review the guidance contained within this document and during the development of agency business continuity plans.

Attachment 1

Interrelationship of the Information Security Framework Policy and Subpolicies

Information Security Framework	Security Requirements								
	Risk Management	Confidentiality	Integrity	Availability	Protect, Detect and Respond	Identification & Authentication	Access Control & Authorization	Security Audit Logging	Security Management & Administration
Information Security Framework Policy Sections	5.1	5.2	5.2	5.2	5.3	5.4	5.5	5.6	5.7
SUBPOLICIES									
Boundary Security (B.2)	X			X	X	X	X	X	X
Data Classification (B.11)	X	X	X	X	X	X	X	X	X
Disposal, Servicing and Transfer of IT Equipment (E.1)	X	X							X
Internet Security (B.6)	X					X	X		X
Intrusion Prevention and Detection (B.12)	X		X		X		X	X	X
Malicious Code Security (B.4)	X		X		X				X
Password & PIN Security (B.3)	X	X			X	X	X	X	X
Portable Computing Security (B.9)	X	X				X	X	X	X
Remote Access Security (B.5)	X	X		X		X	X	X	X
Security Education and Awareness (B.8)	X	X	X	X	X	X	X	X	X
Security Incident Response (B.7)	X		X	X	X			X	X
Security Notifications (B.10)	X	X			X	X	X		X