# Information Security Aspects of Business Continuity Planning Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure that information security is properly addressed within the organization’s Business Continuity Planning (BCP) strategy.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Information Security Aspects of Business Continuity Planning Policy applies to all business processes and data, information systems and components, personnel, and physical areas of [Insert Company’s Name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws, Regulations, and Standards

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| ISO27001:2013 | A.17 (A.17.1, A.17.2) |
| NIST SP 800-53 v4 | CP-1, CP-2, CP-4, PM-9, RA-3, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13  |

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

**Information Security Continuity Management:**

* The organization will determine its requirements for information security and how it fits into the overall continuity of information security management in crises.
	+ Including aspects like purpose, roles, and responsibilities.
* The organization will create, document, and implement any processes and controls related to the continuity for information security during crisis situations.
	+ Contingency plans will go through testing to ensure comprehensiveness and effectiveness.
* These information security processes and controls will be reviewed and validated regularly to ensure their continued effectiveness.

**Security Contingency Planning within the context of enterprise BCP:**

* [Insert Company’s Name] should conduct a Business Impact Analysis (BIA) to identify security functions, processes, and applications that are critical to [Insert Company’s Name] and determine a point in time (i.e. recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to [Insert Company’s Name].
* [Insert Company’s Name] should utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical security functions, processes, and applications.
* [Insert Company’s Name] should assign contingency roles and responsibilities to key individuals from all security functions.
* [Insert Company’s Name] should establish procedures to maintain continuity of critical security functions despite critical information system disruption, breach, or failure.
* [Insert Company’s Name] should document a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable [Insert Company’s Name] to respond to potential disruptions and recover its critical security functions within a predetermined RTO following a disruption.
* [Insert Company’s Name] should establish a process to ensure that the BCP is reviewed and approved by senior management.
* [Insert Company’s Name] should distribute copies of the BCP to key personnel responsible for the recovery of the critical security functions and other relevant personnel and partners with contingency roles, as determined by [Insert Company’s Name].
* Sufficient redundancies will be implemented to ensure availability requirements are met.

**Data Backups:**

* [Insert Company’s Name] should develop, maintain, and document data backup and storage procedures to ensure the recovery of electronic information in the event of failure.
* [Insert Company’s Name] should identify and apply security requirements for protecting data backups based on the different types of data (sensitive, confidential, public) handled by the entity.
* [Insert Company’s Name] should establish a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.