SNOWBE ONLINE Policy#CM-3 Configuration Change Control

**Michael Kohronas:**

**<Configuration Change Control>**

**Version #3**

**DATE: 06/2024**

Table of Contents

[Policy 2](#_Toc170657955)

[Scope 2](#_Toc170657956)

[Definitions 2](#_Toc170657957)

[Roles & Responsibilities 3](#_Toc170657958)

[Policy 3](#_Toc170657959)

[Exceptions/Exemptions 4](#_Toc170657960)

[Enforcement 5](#_Toc170657961)

[Version History Table 5](#_Toc170657962)

[Citations 6](#_Toc170657963)

Policy

The purpose of the SnowBe Change Management/Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to SnowBe Information Resources.

Scope

The SnowBe Change Management/Control Policy applies to any individual, entity, or process that create, evaluate, and/or implement changes to SnowBes Information Resource.

Definitions

**Change:** A Change is defined by an addition, modification, or removal of configuration item that could have an effect on IT Services and which is approved by management, enhances business process changes (fixes) and minimize risk to IT Services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

**Change Authority –** The person or group authorizing a change.

**Change Management -** Change Management refers to the process used to control the lifecycle of all changes.

**Change Management Policy -** Change Management Policy is the guiding standard that describes the procedures for, and specifies the rules and levels of authorization required to approve, different types of Changes.

**Change Management Log Report –** Log that is maintained by IT Staff Members related to changes in the IT Environment.

**Change History –** Information of changes for historical purposes, for example, what was done, when it was done, by whom and why.

**Emergency Change**: An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs).

**Normal Change:** A Normal Change is a change that does not have a pre-approved SOP and is not classified as an Emergency Change; it follows the full Change Management Process and have a predefined maintenance window.

**Request for Change (RFC):** A formal proposal for an alteration to any component of the IT infrastructure or any aspect of IT services.

**Standard Change:** A Standard Change is a pre-authorized change that is low-risk, predictable in its outcome and repeatable through defined work instructions in a standard operating procedure (SOP).

Roles & Responsibilities

**All Employees, contractors, or interns –** All employees are required to go through change management when making changes to any of the following systems listed in the policy below.

**CISO –** Oversees the creation of change management procedures and management/usage of it.

**IT Security team –** Creates the change management processes and procedures, manage the change management processes by overlooking change forms and validating them for integrity.

# Policy

This policy formalizes the requirements for changes within the Information Technology environment. The change procedures are designed with the size and complexity of the environment in mind. The change process includes provisions that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

Change management generally includes the following steps:

* Planning: Plan the change, including the implementation design, schedule, communication plan, test plan, and roll back plan.
* Evaluation: Evaluate the change, including determining the risk based in priority level of service and the nature of
* the proposed change, determining the change type and the change process to use.
* Review: Review the change plan with peers and/or appropriate change authority as determined by the type of change.
* Communication: Communicate about changes with the appropriate parties (targeted or campus-wide).
* Implementation: Implement the change.
* Documentation: Document the change and any review and approval information.
* Post-change review: Review the change with an eye to future improvements.

This policy applies to all changes to architectures, tools, and IT services provided by the Office of Information Technology. Modifications made to non-production systems (such as testing environments with no impact on production IT Services) are outside the scope of this policy.

Staff maintaining systems and network systems are required to document changes. The Office of Information Technology

staff will record changes for the following categories of the IT Environment:

* Firewall
* Telephony/Teams environments (including audio codes)
* Network equipment (including Wireless Access Points (WAP))
* Servers, including new installation and patches
* Administrative and Academic Systems
* Mobile Apps
* Liquidation/Destruction of Hard Drives
* PCI Network
* Cash Registers
* NOC Access
* Internal Risk Assessment
* Penetration Network Tests
* Network monitoring/BitLyft

Types of Changes:

There are three types of changes: (a) a standard change, (b) a normal change (of low, medium, or high risk), and (c) an Emergency Change.

**Standard –** A repeatable change that has been pre-authorized by the Change Authority by means of a documented

procedure that controls risk and has predictable outcomes.

**Normal –** a change that is not an emergency change or a standard change. Normal changes follow the defined steps of

the change management process. Low, Medium, or High priority is determined by the Change Authority, IT or delegates

according to the Risk Assessment Instrument included below.

a. Normal Low Changes must be reviewed and approved by the change authority.

b. Normal Medium Changes must be reviewed and approved by the Change Authority and unit director or system

Owner.

c. Normal High Changes must be approved by the IT Executive Team as Change Authority.

**Emergency Change** – A change that must be introduced as soon as possible due to likely negative service impacts. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps due to the urgent nature of the issue; however, any Emergency Change must still be authorized by a IT Executive.

Risk Assessment Instrument: Risk and Change Type Matrix for Normal and Emergency Changes.

* Determine the impact of the change to the service.
* Then assess the urgency of the proposed change (low can generally wait, Medium, cannot, and high needs to be done ASAP)
* The matrix shows whether the type of change is then a Normal Low, Normal Medium, Normal High, or an Emergency Change (Note: A Standard change does not need to use this matrix because risk is controlled by a
* pre-approved standardized process)

Changes to production systems are made only by authorized individuals in a controlled manner.

Exceptions/Exemptions

Exceptions to this Policy will be considered on a case-by-case basis and do not guarantee approval. To request an exception, please submit a written request to the IT Director outlining the following:

How to Request Exceptions/Exemptions?

To request an Exception or Exemption from a Policy that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The IT Director, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions. Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement

The failure to comply with policies, Policys, or Policys will result in a warning or disciplinary action depending on the severity of the infraction.

Version History Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version #** | **Implementation Date** | **Document Owner** | **Approved By** | **Description** |
| v1 | 06/06/2024 | Michael Kohronas |  | Added the exception and exemption and enforcement as a group |
| V2 | 06/07/2024 | Michael Kohronas |  | Fixed issues with text size and font, added name and date to header, |
| V3 | 06/24/2024 | Michael Kohronas |  | Added the change management control policy information |

Citations

<https://frsecure.com/change-management-policy-template/>

<https://www.doa.la.gov/media/lhibcody/ots_change_management_policy.pdf>

<https://www.mountunion.edu/Documents/Hidden%20Pages/University%20Policies/Technology/IT%20Change%20Management%20Policy.pdf>