Status: ☑ Working Draft ☐ Approved ☐ Adopted

Document owner: Ian Corbitt - SnowBe

1/27/2023

ITP107 Change Control Policy

Purpose
The purpose of this policy is to ensure that all changes to SnowBe IT Resources minimize any potential negative impact on services and Users.

Scope
This IT policy, and all policies referenced herein, shall apply to SnowBe employees, guests, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, SnowBe's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions
SnowBe utilizes various industries' standard definitions compiled and managed SnowBe Information Technology for all information security and privacy. Refer to SnowBe IT Document ITD002, Technical Definitions.

Terms key to this policy:

Change Control: a systematic approach to managing all changes to SnowBe IT Resources. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted, and that resources are used efficiently.

IT Resources: All computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and related materials and services.

Roles and Responsibilities
Functional Officer - Chief Information Security Officer: Overall owner of SnowBe's IT Security subdivision and all its assets. Tasked with ensuring all IT assets are secured in accordance with this and all applicable laws, regulations, and business policies.

Responsible Officer - Chief Information Officer: Overall owner of SnowBe's IT division and all its assets.

ITP107 Change Control Policy V 1.1

Status: ☑ Working Draft ☐ Approved ☐ Adopted

Document owner: Ian Corbitt - SnowBe

1/27/2023

Policy

- All SnowBe IT Resources changes must be documented per the Change Control Process.
- All changes to SnowBe IT Resources must follow the Change Control Process to ensure appropriate approval, planning, and execution.
- Change requests may not be required for non-production (e.g., DEV, Test, QA) environments unless there is a significant upgrade or an impact.
- Production change requests must note that the change has been successfully applied, tested, and verified in a non-production environment when a suitable environment(s) exists.
- Changes to production environments undergo impact examination before submitting the change request per the Change Control Process. This information will be used to determine the impact of the change by considering:
  - The impact the proposed change will have on business services if it is expected to cause a widespread outage, a loss of connectivity, or functionality to a specific group or groups.
  - The risk involved in not making the change;
  - The risk if the change does not go as planned; and
  - Predictability of the success of the change.
- Changes must be vetted for security implications through Information Security and Assurance (ISA) participation.
- Significant User experience changes must be conveyed to the Change Control Board (CCB) and communicated to the affected audience and IT Service Desk Level 1.
- A "lessons learned" session should occur in the event of an incident during a change request.

Exceptions/Exemptions

Exceptions or exemptions for this policy to this policy are reviewed and enacted on a case-by-case basis. For further details on obtaining an exception or exemption from this policy, refer to SnowBe IT Policy ITP042, IT Policy Exceptions and Exemptions.

Enforcement

This policy is self-enforcing by the authority granted to it by all local and federal laws as well as SnowBe business operations policies and SnowBe IT Policy ITP100. This policy must be adhered to except in the exceptions and exemptions noted above or in SnowBe Document ITD-001 IT Exceptions and Exemptions, otherwise one or more of the following actions may result:

- Written warning regarding policy violation.
- Disciplinary action, up to and including termination.
- Legal action taken against the individual(s) outside of compliance.

Status: ☑ Working Draft ☐ Approved ☐ Adopted

Document owner: Ian Corbitt - SnowBe

1/27/2023

Version History

Version	Date	Owner	Approved	Description
1.0	*1/20/2023*	*Ian Corbitt*	*Prostetnic Vogon Jeltz*	*Initial Release*
1.1	*1/20/2023*	*Ian Corbitt*	*Prostetnic Vogon Jeltz*	*Minor editorial changes*

Citations

[Fordham University – Information Technology: Change Control Policy](#)