



SNOWBE ONLINE Policy# 3

Incident Response

Your name: Tyrall Waller

Group 6 Section 01

Draft - Version # 1.1

DATE: 3/10/25



Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

POLICY 3

EXCEPTIONS/EXEMPTIONS 4

ENFORCEMENT 4

VERSION HISTORY TABLE 6

CITATIONS 7

Purpose

The purpose of this policy is to manage all security incidents. This policy will mandate the activities and actions carried out by the personnel of this organization. In the event of an incident, organized procedures are put in place to ensure the proper steps are known and executed in response efficiently, consistently, and effectively. The incident Response Policy ensure all hands are prepared to address any threats in a timely manner and able to provide protection from the incident escalating to cause additional damage or harm while ensuring the requirements are being met for compliance.

Scope

The Incident Response Policy focuses on identification, management, and Security incident resolution. This policy applies to company personnel employed and or associated with via contract and third-party. Policy designates full responsibility to the Cyber Incident Response Team to manage and serve as the primary for all incidents. Escalation, notification, and communication is outlined in different processes relevant to the organization and identified and associated parties who are external to the organization's personnel.

Definitions

Data Breach: Unauthorized access, acquisition, use or disclosure of restricted data. Data breach notifications are subject to regulatory requirements following a privacy investigation and risk assessment.

Incident: An event, electronic, physical or social that adversely impacts the confidentiality, integrity or availability of data or information systems, real or suspected action, inconsistent with privacy or acceptable use policies.

Information System: A collection of hardware, software, data, people, and processes that work together to gather, store, analyze, and share information.

Roles & Responsibilities

Employees:

Must read and understand the policies and procedures that are put in place.

Responsible for recognizing and reporting potential security incidents and suspicious activity to the Incident Response Manager and the Information Technology Team.

Required to receive up to date training on how to identify potential threats and handling procedures to take if suspicious activity has taken place.

Must comply with all relevant laws, regulations and internal policies related to incident response.

Incident Response Team:

Document all activity that occurs during an incident. (People involved, Actions taken in response, and the after action report)

Communicate the incident and resolution to the required authority and all hands personnel.

Incident Manager:

Responsible for managing incidents, coordinating response efforts, and ensuring procedures put in place are available and followed to resolve the issue.

Communication Lead:

Manages all internal and external communication related to each incident, ensuring that information is accurately and effectively shared.

Technical Support:

Investigate and diagnose all incidents, working alongside the Incident Response Team to identify the root cause and implement solutions.

Security and Service Analyst:

Handle initial reports and incidents, escalating them to the appropriate section for handling purposes.

Monitor security systems, identify potential threats, and assist incident investigations.

Policy

The implementation of policies, standard procedures, and guidelines enable the ability to manage, execute, protect and support all business activity and production in support of this organization and its infrastructure. By defining and managing incident response with productive procedures put in place, this policy aims to produce nothing less the high quality effective management, response, and protection while aiming to ensure legal requirement and compliance are being met as the end result.

Section leaders gather documented performance of threat activity that drive action to make policy changes, training and decisions concerning effective incident response. Established procedures of identifying threat management and resolutions will determine the effectiveness of all incident response

matters.

Exceptions/Exemptions

To ensure flexibility in security implementation while maintaining strong controls, the following exception/exemption policy applies:

1. Request Process:

a. Any request for an exception/exemption must be submitted in writing to the IT Security Manager.

b. The request must outline the reason, the systems affected, and the duration required.

2. Justification: The request must provide a valid business or operational reason that necessitates an exception.

3. Approval Authority: Approval must be granted by both the IT Security Manager

4. Duration:

a. Exceptions/exemptions will be granted for a limited period, subject to review every 6 months.

b. If an extension is required, a new request must be submitted along with the previous action provided.

Enforcement

A discharge by an employer of an individual for violation of an employer rule is for misconduct connected with the work if the rule is reasonable, the individual knew or should have known the rule, and the violation is willful or wanton, material, and substantially injures or tends to injure the employer's interests.

If the individual has previously violated a minor employer rule or has previously violated the same or a similar employer rule with the knowledge of the employer, a discharge is for misconduct connected with the work if the violation substantially injures or tends to injure the employer's interests and has been preceded by prior warnings or reprimands for previous violations, or if the individual's course of conduct as a whole demonstrates a substantial disregard of the employer's interests following prior warnings or reprimands for violations of other employer rules.

Thus, a violation of an employer rule is not, by itself, misconduct. It would be misconduct if all of the following conditions are met:

The rule is reasonable.
The claimant knew or should have known the rule.
The violation is willful and wanton.

NOTE: Violation of a reasonable employer rule is not willful if the claimant has shown good cause for violating the rule.

The violation is material.
The violation substantially injures or tends to injure the employer's interests.
The employer has warned or reprimanded the claimant for previous violations of the same or similar employer rules.

Reasonable Rule

It is the employer's right generally to establish such rules for his or her employees as, in the employer's opinion, are necessary for the proper conduct of his or her business. Violation of an employer rule regarding the performance of the work will generally be a violation of a reasonable rule.

1. Knowledge of Rule

To be known, a rule must have been disseminated generally to all employees or made known to the claimant individually, either orally or in writing. If a claimant has been given a written copy of employer rules (as in an employee handbook), his or her failure to read the rules would not render the discharge for reasons other than misconduct. If the claimant was never informed of the existence of the employer rule, the discharge for violating the rule would generally not be for misconduct.

Some employer rules, however, do not need to be transmitted to the employee but are implied or are known rules in the occupation or industry. For example, there does not need to be a written employer rule against stealing of employer property or a formal employer rule that an employee in a bank does not drink on the job.

2. Violation is Willful

If a claimant has good cause for his or her violation of a rule, or if the violation is due to mere inefficiency, unsatisfactory conduct, failure in good performance as the result of inability or incapacity, inadvertence or ordinary negligence in isolated instances, or good faith errors in judgment or discretion, then there is no misconduct. Under such circumstances, the violation of the rule would not be a wilful, deliberate, or flagrant violation.

3. Materiality of Rule Violation

Violation of an employer rule is material when the employer's operations are interfered with.

4. Substantial Injury to Employer's Interest

From the definition of a "reasonable employer rule," it follows that any violation of a reasonable rule will injure or tend to injure the employer's interests. However, there is no misconduct unless the injury or tendency to injure is substantial.

5. Warnings and Reprimands

Some employer rules are such that their first violations would be misconduct, for example, rules prohibiting fighting or drinking on the job. Warnings and reprimands need not be considered for this kind of violations.

However, if the claimant has broken an employer rule which, although reasonable, is of comparatively slight significance, the claimant should be entitled to a warning or reprimand so that he or she would have the opportunity of mending ways before he or she was discharged. Therefore, if the employer has a rule about tardiness, or overstaying coffee-breaks, or any of the more minor conditions of employment, to constitute misconduct the employer would need to show that the claimant persisted in violating the rule despite warnings and/or reprimands.

What if the warnings or reprimands were not for the same type violations as the one which occasioned the claimant's discharge? Even so, the discharge would be for misconduct if the claimant's conduct, viewed in its entirety, evinced a deliberate disregard of the employer's interests. For example, a claimant may have been warned several times over a period of two or three months because of such violations as arguing with coworkers, wandering away from the workstation to engage in conversations, and failure to follow instructions. If, shortly after the last warning, the claimant violated an employer rule relative to tardiness by appearing at work 20 minutes late without good cause and was thereupon discharged, the discharge would be for misconduct.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	3/10/25	Tyrall Waller	Tyrall Waller	Incident Response Policy

Citations

What is an incident Response Policy and How to Create one?

(BlueVoyant, 2025)

<https://www.bluevoyant.com/knowledge-center/what-is-an-incident-response-policy-and-how-to-create-one#incident-response-policy-purpose-and-scope>

Incident Response Policy

(Regulation and Policy Hub, Feb 2020)

<https://policy.ufl.edu/policy/incident-response-policy/>

Computer Security Incident Response Team

(University of Florida, 2025)

<https://it.ufl.edu/security/security-guidance/incident-response-procedures/computer-security-incident-response-team/>

Incident Response Process: The 6 Steps and How to Test They Work

(BlueVoyant, 2025)

<https://www.bluevoyant.com/knowledge-center/incident-response-process-the-6-steps-and-how-to-test-they-work>