gravyty

your force for good

Incident Management Policy
Version No: 1.4

Version 1.4 | 2023

Table of Contents

1. Overview

1.1. Information security events and incidents can pose significant risks when not handled appropriately. Handling information security incidents should involve timely reporting, reactive activities as well as preventive activities and the implementation of a lesson-learned process leading to related risk mitigation. Incident response guidelines should be created in a manner that ensures information security events and weaknesses associated with information systems are reported and dealt with appropriately.

2. Purpose

2.1. The purpose of this policy is to:

- Provide clear guidelines for information security decision makers regarding how to act when an information security incident occurs, how to report it and which parameters should be considered in the decision-making process.
- Set up a regulated process of reporting to relevant factors in the case of an information security incident.
- Set up an orderly process of drawing conclusions, to prevent the recurrence of such incidents and record them for future reference and analysis.

3. Scope

3.1. This policy applies to all events and incidents occurring in Gravyty's systems or reported by Gravyty's employees.

4. General

4.1. Every Gravyty employee has the obligation to report any suspicion of an irregular event if there is a reasonable basis for believing that an unauthorized activity is being carried out in their surroundings or in the company's systems.

4.2. Every Gravyty employee should be alert and pay attention to suspicious activities in their work environment.

5. Incident Handling Guidelines

5.1. Security-related events

5.1.1. Security-related events are to be reported to the IT Management Group. Corrective measures will be prescribed as needed.

5.1.2. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences

5.2. Security incident handling

5.2.1. Once an event turns out to be an incident, it is to be handled by the information security manager, who is to act to minimize the impact and to mitigate all related risks, keeping Gravyty's management updated in the process.

5.2.2. Every information security incident, from the moment of its announcement, is to conclude with an exhaustive report which is to specify the following:

- Incident detection
- Response to the incident
- Neutralizing the endangering factors
- Drawing conclusions
- Documentation
- Lesson Learned