**Name of Organization**

**Incident Categorization**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Categorization is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc88583086)

[II. Guidelines 5](#_Toc88583087)

[Table 1: General Guidelines for Incident Prioritization 7](#_Toc88583088)

[Table 2: Most common Incidents and their classification level 8](#_Toc88583089)

[III. Supporting Information 10](#_Toc88583090)

# Introduction and Purpose

This document defines objectives for establishing specific standards for the categorization of cyber security incidents.

Incident Categorization builds on the objectives established in the Incident Response Plan (“the Plan”) and provides appropriate prioritization of incidents. It will help develop metrics for future remediation and focuses on classifying the incident at the appropriate level (category, type, and priority) to support incident management prioritization. Incident classification may change frequently during the incident management lifecycle as the team learns more about the incident from the analysis being performed over time.

This Incident Categorization is based on NIST and FIPS PUB 199 (Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems).

# Guidelines

FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

Table 1 below provides guidelines on what criteria to use to assign appropriate prioritization to specific incidents. For each categorization, the scope of the incident also must be taken into consideration by determining the overall risk, which includes evaluation of affected users, asset criticality and locations (e.g., a virus outbreak in entire test environment, completely isolated from production will have a lower categorization than the same virus outbreak in production with customer data and critical business assets).

Table 2 below provides an overview of most common incidents and their standard categorization. Note - the overall risk of the event including affected users, asset criticality and locations needs to be considered – categorization may require to be changed. The Incident Commander is responsible of setting the correct category for each Incident. Consistent case classification is required for the Cybersecurity Incident Response Team (CIRT) to provide accurate reporting to management on a regular basis. In addition, the classifications will provide Incident Commanders with proper case handling procedures and will form the basis of Service Level Agreements (SLA’s) between the CIRT and other Organizational departments.

It is critical that the CIRT also provide consistent and timely response to the customer based on categorization, and that sensitive information is handled appropriately.

## Table 1: General Guidelines for Incident Prioritization

|  |  |  |
| --- | --- | --- |
| **Description** | **Priority level** | **Category** |
| A security incident will be assigned as “Priority Level 1/High” is the incident is characterized by the following:− The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.  | P1 | **High** |
| A security incident will be assigned as “Priority Level 2/Moderate” is the incident is characterized by the following:− The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.  | P2 | **Moderate** |
| A security incident will be assigned as “Priority Level 3/Low” if the incident is characterized by the following:− The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.2 AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.  | P3 | **Low** |

## Table 2: Most common Incidents and their classification level

| Class | Type | Priority | Description |
| --- | --- | --- | --- |
| Abusive Content | Spam | P3 | Unsolicited email |
| Harassment | P2 | Discrediting and discriminating against somebody (i.e., Cyberstalking) |
| Inappropriate Content | P3 | Glorification of violence, hate speech, etc. |
| Illegal Pornography | P1 | All types of illegal pornography. Child pornography need special reporting to legal authorities (Human Resource & Legal have to be involved)  |
| Malicious Code | Virus | P2 | Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code. |
| Crypto Miner | P1 |
| Worm | P1 |
| Trojan | P2 |
| Spyware | P3 |
| Ransomware | P1 |
| Information Gathering | Scanning | P2 | Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts |
| Sniffing | P1 | Observing and recording network traffic |
| Social Engineering | P2 | Gathering information from a human being in a non-technical way (e.g., Phishing, lies, tricks like phone calls, bribes, or threats) |
| Intrusion Attempts | Exploiting known vulnerabilities | P1 | An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier with standard names (e.g., buffer overflow, backdoors, cross side scripting, etc.). |
| Login attempts | P2 | Multiple login attempts (guessing / cracking of passwords, brute force) |
| Unknown vulnerabilities | P1 | An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities that are still unclassified |
| Intrusion | Privileged account compromise | P1 | A successful compromise of a system or application (service). This can have been caused remotely or locally by a known or new vulnerability |
| Unprivileged account compromise | P2 |
| Application compromise | P1 |
| Availability | DoS | P1 | In this kind of attack a system is bombarded with so many packets that the operations are delayed or the system crashes. However, availability can also be affected by local actions (repeated transactions, destruction, disruption of power supply, etc.). |
| DDoS | P1 |
| Sabotage | P1 |
| Information Security | Unauthorized access to information | P1 | Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information remotely or locally during transmission (‘man in the middle’: wiretapping, spoofing or hijacking) are possible. |
| Unauthorized modification of information | P1 |
| Fraud | Unauthorized use of resources | P3 | Using resources for unauthorized purposes including profit-making ventures (e.g., the use of e-mail to participate in illegal profit chain letters or pyramid schemes) |
| Copyright Infringement | P3 | Selling or using copies of unlicensed commercial software or other copyright protected materials (Warez, Graphics, Photos etc.) |
| Masquerade | P1 | Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it (e.g., Using accounts from other persons) |
| Physical Security and Safety | IT-System failures | P1 | Technical failure of an IT-System which results into failure of IT-Operations |
| Lightning | P1 | Technical failure through lightning strikes |
| Fire | P1 | Direct damage caused by fire |
| Water | P2 | Direct damage caused by rain, floods, disruption of water supply, defects in the heating installation, defects in air conditioning systems, sprinkler systems, fire-fighting systems or sabotage through water. |
| Cable failures | P2 | Fire in Cables, wrong Cabling  |
| Inadmissible temperature | P2 | Direct damage through rise or fall of the required operational temperature. |
| Magnetic fields | P2 | Loss of data through magnetic fields |
| Dust or dirt | P2 | Direct damage through dust or dirt influence |
| Riots | P2 | Any threat / direct damage through public unrest |
| Nuclear emergency | P1 | Any threat / direct damage through nuclear emergencies |
| Earthquakes | P2 | Any threat / direct damage through earthquakes (seismic activity) |
| Theft / Loss | Notebook/ Tablet | P2 | Theft / loss of various mobile devices regardless if these devices are protected by encryption software and / or remote wipe schemes. |
| Desktop |
| Removable Storage/USB |
| Phone |
| Policy Violation | Unacceptable use | P2 | Using any IT System in ways which violate the current Organization Information Security Policy. |
| Other | Not defined | N/A | All Events / Incidents which do not fit in one of the given categories should be put into this class. If the number of Incidents in this class increases, it is an indicator that the classification scheme has to be revised. |

# Supporting Information

[**DOI FIPS 199 Workbook**](https://communities.geoplatform.gov/gpcustomers/wp-content/uploads/2018/02/DOI-FIPS-199-Workbook.xls)- <https://communities.geoplatform.gov/gpcustomers/wp-content/uploads/2018/02/DOI-FIPS-199-Workbook.xls>

**FIPS PUB 200** - https://csrc.nist.gov/publications/detail/fips/200/final