Vulnerability Management

Resource reference: **VPS-33-D04**
Status: **Approved**
Last revision: **2023-12-19**

Introduction

This directive defines a standard for all Concordia community members to follow to support the Coordinated Vulnerability Disclosure (CVD) and Vulnerability Management (VM) processes at Concordia University.

Concordia's Chief Information Security Officer has issued this directive under the authority of Policy Number: VPS-33 - Information Security Policy.

Questions about this directive may be referred to: ciso@concordia.ca.

Definitions

Vulnerability: Vulnerability is a weakness in a computer system, network, or application that can be exploited by attackers to gain unauthorized access, steal data, disrupt operations, or carry out other malicious activities.

Threat: Threat refers to any potential danger or harmful event that can exploit vulnerabilities in a system or organization, leading to damage, unauthorized access, data breaches, or disruption of operations.

Exploit: Exploit refers to a piece of software, a sequence of commands, or a set of techniques used to take advantage of a vulnerability in a computer system, application, or network.

Risk: Risk generally refers to the likelihood or probability of an adverse event occurring and the potential consequences or impact associated with that event.

Patch: Patch refers to a software update or modification designed to fix security vulnerabilities or address other security-related issues in a computer program, operating system, or application.

CVSS: CVSS stands for Common Vulnerability Scoring System, and it is a framework for assessing and communicating the severity of security vulnerabilities in software.

Sensitive Data: Sensitive data refers to data or details that, if disclosed or compromised, could have adverse consequences for individuals, institutions, or both.

Sensitive data within a university setting may include, but is not limited to:

Personal Identifiable Information (PII), Academic Records, Financial Information, Research Data, Health Records, IT Systems Access Credentials, Student and Alumni Records, Intellectual Property, etc.

Coordinated Vulnerability Disclosure (CVD): The process of responsibly disclosing and addressing security vulnerabilities in a coordinated manner. This involves reporting vulnerabilities to the appropriate parties and working collaboratively to mitigate risks without undue public exposure.

IT Staff: Any staff member responsible for managing an organization's information technology infrastructure, including system owners and administrators, database (DB) administrators, network administrators, analysts, technicians, operators, managers, application developers, coordinators, and architects.

Scope

This directive applies to all University digital assets including but not limited to information systems, network infrastructure, servers, desktop computers, laptops, mobile devices, operating systems, etc. It includes both cloud-based and on-premise solutions across all departments and units for all Concordia owned assets.

Objective

The objective of this directive is to establish a standardized approach for vulnerability management at Concordia University including definition of the Coordinated Vulnerability Disclosure (CVD) and Vulnerability Management (VM) processes which include the following goals:

- Adopt an integrated approach to vulnerability management that covers all Concordia University departments and units.
- Align with the principles of the Quebec government's "Processus de gestion des menaces, des vulnerabilities, et des incidents" (GMVI) processes including collaboration, clear roles and responsibilities, escalation procedures, and continuous improvement.
- Establish cross-functional collaboration and coordination between departments to ensure a holistic and unified response to vulnerabilities.
- Establish a tiered approach to vulnerability management coordination, with different levels based on vulnerabilities' severity and potential impact.
- Provide a methodology to identify and prioritize vulnerabilities within the university's information systems and infrastructure.
- Implement appropriate controls and measures to mitigate identified vulnerabilities.
- Achieve full resolution of vulnerabilities
- Foster a culture of proactive vulnerability management to enhance the university's overall security posture.
- Specify the levels of coordination and communications applicable.

Roles and Responsibilities

Chief Information Security Officer (CISO):

- Approve, oversee and ensure the implementation of the Coordinated Vulnerability Disclosure (CVD) and Vulnerability Management (VM) processes and associated directives.
- Develops and maintains appropriate strategic and operational plans for the IITS Security Team.

IITS Security Team:

- Lead and operate the Coordinated Vulnerability Disclosure (CVD) and Vulnerability Management (VM) processes University-wide.
- Identify and analyze vulnerabilities using industry-standard tools and methodologies.
- Own, maintain and operate Concordia's single University-wide vulnerability management register.
- Prioritize vulnerabilities based on their severity, impact, and exploitability.
- Coordinate with system owners, administrators, and other IT staff to remediate identified vulnerabilities.
- Regularly report on the security posture and mitigation efforts to CISO.
- Share potential vulnerabilities on assets to Concordia's cybersecurity ecosystem through the dedicated team's channels (Cybersecurity Operations).

IT Staff:

- Participate and comply to the University-wide Coordinated Vulnerability Disclosure (CVD) and Vulnerability Management (VM) processes.
- Report all identified vulnerabilities to the IITS Security Team and contribute to the maintenance of an accurate and up-to-date Vulnerability Register.
- Maintain a registry of systems and applications under their responsibility.
- Remediate vulnerabilities within prescribed timelines.
- Implement appropriate remediating security controls and patches to mitigate vulnerabilities.

Coordinated Vulnerability Disclosure (CVD) Process

Vulnerability identification

Concordia identifies and collects vulnerability reports in three ways:

1. Vulnerability analysis and scans.
2. Monitoring public and private sources of vulnerability information.
3. Direct reports of vulnerabilities:
    a. The IT Staff performs an initial analysis to assess a vulnerability's presence and compares with existing reports to identify duplicates.
    b. All identified vulnerabilities must be reported immediately to soc@concordia.ca

Vulnerability logging

Collected vulnerabilities that were identified through various channels such as direct reporting, vulnerability scanning tools, penetration testing, and security audits must be logged into the vulnerability register. All relevant information should be added including at least the following:

- Vulnerability Name
- Description
- Discovery Date
- Affected assets
- System Criticality
- Confirmed fix and or/ mitigation measures

Mitigation, co-ordination and assistance

The system owner is responsible for coordinating the remediation or the implementation of mitigation measures with the concerned IT Staff, external partners, and all other stakeholders, and follow Concordia's vulnerability management (VM) process.

Vulnerability Management (VM) Process

1. Determine potential damage or level of impact

For each vulnerability identified and logged, the IITS Security Team collaborates with the system owner or administrator to evaluate the potential damage or level of impact the vulnerability could have on Concordia's systems, data, and operations.

There are both technical factors and university operations factors to consider when evaluating the impact of an exploited vulnerability:

- **Technical Impact Factors**

Estimates the magnitude of the impact on the system if the vulnerability were to be exploited:

	Low	**Medium**	**High**	**Critical**
Loss of Confidentiality - How much data could be disclosed and how sensitive is it?	Minimal non-sensitive data disclosed	Minimal critical data disclosed, extensive non-sensitive data disclosed	Extensive critical data disclosed	All data disclosed
Loss of Integrity - How much data could be corrupted and how damaged is it?	Minimal corrupt data	Extensive slightly corrupt data	Extensive seriously corrupt data	All data totally corrupt
Loss of Availability - How much service could be lost and how vital is it?	Minimal secondary services interrupted	Minimal primary services interrupted; extensive secondary services interrupted	Extensive primary services interrupted	All services completely lost
Loss of Accountability - Are the threat agents' actions traceable to an individual?		Fully traceable	Possibly traceable	Completely anonymous

- **University Operations Impact Factors**

Estimates the magnitude of the impact on the university's operations if the vulnerability were to be exploited:

	Low	Medium	High	Critical
Financial damage - How much financial damage will result from an exploit?	Less than the cost to fix the vulnerability	Minor financial loss	Significant financial loss	Bankruptcy
Reputation damage - Would an exploit result in reputation damage that would harm the University?	Minimal damage	Loss of major accounts	Loss of goodwill	Brand damage
Non-compliance - How much exposure does non-compliance introduce?		Minor violation	Clear violation	High profile violation
Privacy violation - How much personally identifiable information could be disclosed?	One individual	Hundreds of people	Thousands of people	Everyone at the University

Taking both the technical and operations impact factors into consideration, each vulnerability is evaluated as potential low, medium, high, or critical level of impact.

2. Determination of Likelihood/Probability

Evaluate the likelihood or probability of a threat or vulnerability being realized or exploited. Assess the chances of an incident occurring based on factors such as the presence of vulnerabilities, threat actors, or external factors.

There are several factors that can help determine the likelihood.

- **Threat Agent Factors**

The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by threat agent.

	Low	Medium	High	Critical
Skill Level Required - How technically skilled is this group of threat agents?	Security penetration skills	Advanced computer user, Network, and Programming skills	Some technical skills	No technical skills
Motive - How motivated is this group of threat agents to find and exploit this vulnerability?	No reward	Low or no reward	Possible reward	High reward

Opportunity - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability?	Full access or expensive resources required	Special access or resources required	Some access or resources required	No access or resources required
Size - How large is this group of threat agents?	Developers, system administrators	Intranet users, partners	Authenticated users	Anonymous Internet users

- **Vulnerability Factors**

The next set of factors are related to the vulnerability involved. The goal here is to estimate the likelihood of the vulnerability involved being discovered and exploited. Assume the threat agent selected above.

	Low	**Medium**	**High**	**Critical**
Ease of Discovery - How easy is it for this group of threat agents to discover this vulnerability?	Practically impossible	Difficult	Easy	Automated tools available
Ease of Exploit - How easy is it for this group of threat agents to exploit this vulnerability?	Theoretical	Difficult	Easy	Automated tools available
Awareness - How well known is this vulnerability to this group of threat agents?	Unknown	Hidden	Obvious	Knowledge
Intrusion Detection - How likely is an exploit to be detected? Active detection in application	Active detection in application	Logged and reviewed	Logged without review	Not logged

- **Common Vulnerability Scoring System (CVSS) score**

The CVSS 3.1 standard proposed by the Forum of Incident Response and Security Teams (FIRST) is used. A calculation tool is also available: [Common Vulnerability Scoring System Version 3.1 Calculator (first.org).](first.org) The score produced by the tool varies from 0 to 10 and is used to set the initial degree of probability.

	Low	**Medium**	**High**	**Critical**
Calculation with CVSS 3.1 standard				
CVSS Score	0.0 – 3.9	4.0 – 6.9	7.0 – 8.9	9.0 – 10.0

Taking the threat agent and vulnerability factors into consideration alongside the CVSS score, each vulnerability is evaluated as potential low, medium, high, or critical likelihood or exploitation probability.

3. Vulnerability Remediation Timeframe

Following the determination of the potential impact and the likelihood of exploitation, a timeframe or specific remediation timeline for addressing and resolving the vulnerability is established. This ensures that vulnerabilities are promptly remediated to minimize potential risks and ensure Concordia's response is in alignment with the Quebec government's "Processus de gestion des menaces, des vulnerabilities, et des incidents" (GMVI) processes.

Vulnerabilities discovered in development environments are not subject to a remediation timeframe if the following conditions are met:

- The environment does not contain any production data.
- The environment is isolated and cannot establish any communication with the production network.

In all other cases, the IITS Security Team will cross-reference the potential level of impact of the damage (see section - Determine potential damage or impact) and the evaluation of the probability of exploit (see section - Determine the likelihood or probability) to determine the prescribed remediation time to deploy corrective measures.

Prescribed timelines for resolving a vulnerability in an internet-exposed asset with a patch or workaround available:

	Likelihood or probability			
Level of Impact	Low	Medium	High	Critical
Critical	8 days	8 days	8 days	2 days
High	30 days	30 days	8 days	8 days
Medium	60 days	30 days	30 days	30 days
Low	60 days	60 days	60 days	60 days

Prescribed timelines for resolving a vulnerability in an internet-exposed asset with a patch or workaround not available:

	Likelihood or probability			
Level of Impact	Low	Medium	High	Critical
Critical	45 days	15 days	15 days	8 days
High	45 days	45 days	15 days	15 days
Medium	90 days	45 days	45 days	45 days
Low	90 days	90 days	90 days	90 days

Prescribed timelines for resolving a vulnerability in an asset that is not exposed to the internet:

	Likelihood or probability

Level of Impact	Low	Medium	High	Critical
Critical	45 days	30 days	30 days	8 days
High	45 days	45 days	30 days	30 days
Medium	90 days	45 days	45 days	45 days
Low	90 days	90 days	90 days	90 days

Exceptional situations requiring an emergency reaction.

Some situations are considered exceptional and may require emergency urgent actions when one or more of the following criteria are met:

- The Common Vulnerability Score System (CVSS) score is 9 or more.
- The exploit operations require few resources (e.g., unauthenticated user).
- The exploit is active, or the exploit code is publicly available.
- Multiple government agencies are using the product targeted by the vulnerability.

In exceptional situations, mandatory instructions will be transmitted by the CISO for the correction of the vulnerability or for the application of circumvention measures.

4. Vulnerability Remediation Activities and Closure

Once the vulnerability remediation timeframe is established, system owners and administrators must work with the IITS Security Team to identify and implement appropriate risk mitigation strategies such as patching systems, upgrading equipment, or segregating assets on the network. It is the responsibility of the system owners and administrators to implement appropriate remediating security controls and patches to mitigate vulnerabilities.

Following the vulnerability mitigation, the IITS Security team will validate the vulnerability mitigation (eg. run vulnerability scans) and update the corresponding vulnerability record to “closed” in the University-wide vulnerability management register.

Accessibility

Community members with accessibility questions or needs related to this directive are asked to contact the appropriate IITS resource person by emailing iits-accessibility@concordia.ca.

Implementation, Audit, and Review

Concordia’s Chief Information Security Officer (CISO) is responsible for the implementation, review, and approval of this directive. Concordia’s CISO initiates a review as often as necessary, but at least annually, to ensure alignment with both internal and external requirements and regulations.