POL29 - Vulnerability Management Policy

1. Overview

Security vulnerabilities enable attackers to compromise a resource or data. Vulnerabilities occur through product defects, mis-configurations, or gaps in security and IT systems.

Vulnerabilities consist of two categories: unplanned and planned. Unplanned vulnerabilities consist of zero-day vulnerabilities, mis-configurations, and other security mistakes. Planned vulnerabilities consist of known vulnerabilities that cannot, or will not, be fixed.

This vulnerability management policy defines the requirements for Envision Intelligent Solutions Limited (hereinafter know as the Company) IT and security teams to protect company resources from unacceptable risk from unknown and known vulnerabilities. This Vulnerability Management Policy:

- Outlines the expectations, requirements, basic procedures for:
    - Vulnerability Identification
    - Vulnerability Evaluation
    - Vulnerability Mitigation
    - Vulnerability Tracking
- Defines reports to verify compliance with this policy
- Provides penalties for failure to comply with this policy

2. Scope

This policy applies to all Company resources that connect to the organization's network, provide connections between resources, provide security for resources, enable the organization's mission, or host the organization's data. The organization will maintain and track a formal list of resources within the scope of this policy as defined in Appendix I: IT Resource Asset List at the bottom of this document.

Vulnerability management relies on accurate lists of existing systems, software, connections, and security. The scope should be verified as per the asset management policy quarterly to ensure all assets can be accurately assessed and tested for vulnerability identification.

Vulnerability scans may also need to be performed on websites and applications that are not owned and maintained by other departments. The IT Department will need to verify ownership of responsibility for each application and website to ensure no gaps in vulnerability management.

Although critical components of vulnerability management, Patch Management and Change Management will be covered separately in their own Policies.

POL29 - Vulnerability Management Policy

3. Vulnerability Management Policy & Procedure

A. Vulnerability Management Authority

The Chief Information Security Officer (CISO) (currently the General Manager) of the Company is designated as the Vulnerability Management Authority that holds the ultimate responsibility and authority to plan, execute, authorize, or delegate any and all sections of this patch management policy and procedure to internal resources or third-party tools or vendors.

While the Vulnerability Management Authority maintains ultimate responsibility, it is acknowledged that the IT Security Department will generally execute the Vulnerability Management Authority's plans to comply with the Vulnerability Management Policy. The use of "IT Department" elsewhere in this policy refers to the Vulnerability Management Authority, the IT Security Department, and delegated representatives.

The Vulnerability Management Authority also verifies and approves:

- Vulnerability Management Policy Scope
- Vulnerability priority
- Vulnerability and penetration testing
- Any maintenance downtime needed for changes or mitigations
- Any exceptions needed
- Vulnerability management reports
- Enforcement

B. Vulnerability Identification

The IT Department cannot assume that security is invulnerable. Testing must be performed to verify that resources have been installed, configured, integrated, and secured without error or gap in security.

i. Active Vulnerability Detection

Vulnerability scans and penetration testing will be performed quarterly and after significant changes to resources to test for unknown vulnerabilities. High-risk systems containing high-value data or of high importance to operations will require monthly scanning.

Vulnerability scans may be automated and performed with commercial tools as long as the tools can test the specific potential vulnerabilities associated with the resource. Unauthenticated vulnerability scans should be conducted to view the systems from the perspective of an external hacker and authenticated vulnerability scans should be conducted to view systems from the perspective of a hacker with stolen credentials.

Specific vulnerability scans for specific vulnerabilities may be required on an ad hoc basis upon the discovery of specific vulnerabilities or zero-day threats. These scans should be conducted as needed and not constrained to the typical scanning schedule.

POL29 - Vulnerability Management Policy

ii. Information and Threat Monitoring

In addition to testing, the IT Department will continuously monitor and scan a variety of sources to obtain information regarding the release of new attack methods and resource vulnerabilities. Updates and patches for resources fall within the scope of the patch management policy, but unpatched vulnerabilities must be addressed within the scope of this vulnerability management policy. Sources may include, but are not limited to: security mailing lists, vendor notifications, and websites.

iii. Third-Party Systems

The organization will likely require some integration with third party endpoints and systems, such as:

- Leased industrial control systems (elevator systems, fire control systems, etc.)
- Leased operations equipment
- Bring-your-own device (BYOD) equipment brought by employees, consultants, customers, and guests
- Cloud infrastructure jointly monitored and maintained between the cloud vendor and the organization

Vulnerability scans should include all accessible systems connected to the organization and may include these third-party systems. However, the vulnerabilities detected may be beyond the scope of internal resources for resolution. Formal agreements with corporate partners can define responsibilities between the parties for different types of vulnerabilities.

However, regardless of the official responsibility, the IT Department may need to prepare compensating controls to mitigate vulnerabilities. For example, the organization should perform continuous scanning using network access control or equivalent solutions to detect endpoints with vulnerabilities as they attempt to connect to the organization's network and quarantine them.

iv. Documentation

The IT Department must design and document the vulnerability identification program by listing all of the scans, tests, and sources monitored for information. This should be made available as an appendix added to this policy and updated as required. The highest risk assets of the organization must be specifically listed and noted for which tests are performed to verify their status.

When a vulnerability is identified, a ticket will be issued by the IT Department and the vulnerability will be tracked on a Vulnerability Management Tracking list.

C. Vulnerability Evaluation

Once vulnerabilities are identified, they must be verified and evaluated for their potential risk to the organization. The vulnerability should be verified using independent tools and personnel different from the detecting resource. In some cases, an active attempt to exploit the vulnerability may be required to verify the vulnerability or assess its risk.

The vulnerability will be evaluated based upon the following criteria:

- The Common Vulnerability Scoring System (CVSS) Score of the vulnerability (if available)
- The likelihood of the vulnerability being exploited
- Related or cascading vulnerabilities

The CVSS assigns vulnerabilities a score between 1 and 10. The CVSS version 3.0 ratings correspond to:

- 9.0 - 10.0 = Critical Severity
- 7.0 - 8.9 = High Severity
- 4.0 - 6.9 = Medium Severity
- 0.1 - 3.9 = Low Severity
- 0.0 = No Severity (Informational)

These scores do not suggest likelihood of exploitation, but do suggest a level of how much an attacker can affect a system or how much effort may be required.

Similarly, the IT Department needs to evaluate the current environment, the current IT architecture, and the nature of the vulnerability to determine the likelihood of exploitation, which should also be evaluated on a scale from 1 (low likelihood) to 10 (high likelihood). The likeliness of exploitation, where possible, should incorporate threat intelligence information on the exploitation of similar vulnerabilities to support the evaluation. Adding all three of these factors will create a value between 1 (low priority or no action needed) and 20 (urgent action needed) for the vulnerability to be mitigated.

When the vulnerability exposes other existing or new vulnerabilities, those related vulnerabilities should be noted. Related systems, software, and processes should also be noted for the vulnerability.

Generalities are permitted when the list of affected systems is cumbersome, but specifics should be used where possible. For example:

- A vulnerability in the firewall model used in all offices should be generalized as applicable to “all offices, systems, and processes within the organization”
- A vulnerability on a specific router on a specific network segment will specifically list:
    - Range of IP addresses affected
    - Affected people (ex: users in the finance department)
    - Affected devices (ex: finance server, accounting, PCs in the finance department, local printers)
    - Notable or high-value affected processes or systems (ex: accounting systems, accounts payable, accounts receivable, etc.).

D. Vulnerability Priority

Multiple vulnerabilities may be identified in testing or upon the announcement of zero-day vulnerabilities. If necessary, the IT Department will determine the priority for mitigating these vulnerabilities in the context of other existing vulnerabilities using a hierarchy based upon:

- **Evaluated Vulnerability Value** determined during Vulnerability Evaluation (above)
- **Risk Assessment Value** of resources (data, system, process, etc.) affected by the vulnerability to the organization

Risk Assessment Value: The Company uses risk analysis to create a Risk Assessment of internal systems that is recorded and updated in a Risk Register on a scale from 1 (low impact/value) to 10 (highest impact/value). However, a vulnerability may affect multiple systems, software, or processes so the risk value should reflect the total of all resources exposed or the highest exposed risk value, whichever is greater.

When the risk assessment score of 1 to 10 is combined with the vulnerability evaluation rating between 1 and 20, the vulnerability priority score will be generated between 2 (no action needed) and 30 (immediate action required). This prioritization will generally result in tiers of vulnerabilities to be addressed by the IT Department.

E. Vulnerability Mitigation Guidelines

Once a vulnerability has been identified, evaluated, and prioritized, the mitigation to address the vulnerability must be designed, tested, prepared, scheduled, applied, verified, and tested.

i. Vulnerability Mitigation Design

The subcategory of patch management relies upon the application of commercially provided mitigations, or patches, to commercial products and is covered comprehensively in the Patch Management Policy. Broader vulnerability management will require more customization of settings, IT architecture adjustments, and the installation of additional security tools or controls.

Often, there will be several different ways to directly or indirectly mitigate the vulnerability. In many cases complete elimination of the vulnerability will be impossible because of the required cost or complexity of the required mitigation.

However, cost and difficulty may not be used as an excuse to ignore vulnerabilities. Temporary mitigations and partial mitigations (or compensating controls) must be designed, tested, and applied within the time frame appropriate for the level of risk.

Common mitigations include, but are not limited to:

- Deploy mitigating security control such as a new security tool (Firewall, etc.)
- Deploy patches
- Add multi-factor authentication to security controls
- Upgrade or replace vulnerable IT Resource

- Isolate and protect vulnerable IT Resource (network segmentation, disconnect wireless access, etc.)
- Remove or discontinue the use of the IT Resource
- Deploy configuration changes

Complex mitigations may require multiple compensating controls or multiple steps. For more complex mitigations, milestones should be developed to help check progress of implementation.

In some cases mitigation requires the implementation of technical controls that affect users, such as multi factor authentication (MFA). Training on these tools should be considered part of the mitigation design, although training will not generally need to be completed within the minimum vulnerability mitigation schedule timeframe (see below).

ii. Vulnerability Mitigation Testing

For high value resources, the IT Department may decide to test the mitigation in a test environment to check for possible business disruption or other issues. Mitigation that fails the testing process must be redesigned and retested.

iii. Vulnerability Mitigation Preparation

Not all mitigations will be applied successfully or without issue. In some cases a mitigation may render a system unusable or cause cascading problems to other IT systems or software. To prepare for this possibility, the IT Department must ensure that the Disaster Recovery Policy has been executed prior to the Patch Management process.

- A full system backup has been performed prior to the application of the update
- A full data backup has been performed prior to the application of the update

For unsuccessful mitigations that disrupt operations, the IT Department will attempt to roll back the system or software to a previous version to recover functionality. Systems that cannot be rolled back will need to be restored from backup or replaced promptly. In some cases the disruption may leave the system intact and require changes to the mitigation plan to restore operations. Such changes should be implemented as quickly as possible to limit disruption.

The IT Department may attempt multiple times to implement mitigations. For mitigations that cannot be successfully applied, the IT Department must follow the Exception and Mitigation process below.

iv. Vulnerability Mitigation Schedule

Based upon the ranking in the vulnerability management list, the IT Department will be required to pursue mitigation:

- 20+: within 5 business days
- 14.0 - 20: within 10 business days
- 8.0 - 13.9: within 30 business days
- Vulnerabilities ranked below 8.0: within 90 days

Vulnerability mitigation consists of security tools, settings adjustments, IT architecture changes, and other steps needed to lower the risk of a discovered vulnerability.

Other factors affecting the Vulnerability Priority include:

- **Mitigation measures required** to address the vulnerability
- The ability of potential mitigation measure or security control to **address multiple vulnerabilities**
- **Potential business operations disruptions** from required mitigation measures

Mitigation measures required to address the vulnerability can range from simple firewall port adjustments to complex installations of multiple new security tools and controls. In general, simple solutions will be preferred because of the cost of implementation and testing; however, the mitigation must adequately reduce the risk of the exposed vulnerability.

The complexity of the solution does not reduce the urgency to mitigate the vulnerability. However, if temporary measures may be applied to reduce the initial risk, the overall priority and rating of the vulnerability may be re-evaluated.

A potential mitigation measure or security control that **addresses multiple vulnerabilities** may be prioritized at the discretion of the IT Department as long as the mitigation does not interfere with the deployment of more urgent vulnerability mitigations. Efficiency is important but does not outweigh the potential damages of exposed risks.

Potential business operations disruptions may occur because of required mitigation measures. Where possible, business operations should be avoided and minimized.

To avoid excessive disruption, these disruptive mitigations require **Maintenance Windows** need to be scheduled and approved in advance by the Vulnerability Management Authority, preferably with the consent of the appropriate business managers affected by the disruption.

To obtain approval, the IT Department must issue a ticket issued to the Patch Management Authority with the following information in a Maintenance Window request:

- Details regarding affected systems
- Details regarding the urgency of the vulnerability and risk
- Preferred maintenance window and at least one alternative window
- Details regarding rollback procedures should the mitigation fail.

For mitigations required in the absence of the Vulnerability Management Authority, the next available executive in the organization chart can approve the maintenance window.

Should an emergency mitigation need to be applied and no executive can authorize or propose a reasonable alternative maintenance window for the mitigation within the required time frame associated with the urgency of the vulnerability, the IT Department may proceed under the following conditions:

- Documented efforts to obtain approval
- Notify non-executive affected stakeholders (customers, employees, etc.) of the maintenance window
- Proceed with the mitigation without formal approval

It is acknowledged that emergency mitigations and maintenance disruptions may occasionally be required, but the IT Department should always minimize disruption.

v. Vulnerability Mitigation Application

Vulnerability mitigation typically will require a manual process. The IT Department is expected to obtain and deploy sufficient resources to properly establish the mitigation within the expected time frame. When required, outsourced expertise may be obtained to implement mitigations of large scale or for high risk assets.

vi. Vulnerability Mitigation Verification and Testing

Once the mitigation application completes, the IT Department should check that the mitigation works as expected and reduces the risk as intended. Penetration tests and vulnerability scans should be repeated to verify success or to identify and report on unsuccessful mitigations. Vulnerabilities that remain exposed must be addressed as required under Mitigation Tracking and Exceptions (Paragraph 3.F, below).

F. Mitigation Tracking and Exceptions

Mitigations do not always resolve vulnerabilities. In many cases the compensating controls introduced to mitigate a vulnerability shield the vulnerability behind additional layers of security without addressing the vulnerability directly.

All unresolved vulnerabilities and the associated mitigating controls will continue to be tracked and monitored for future potential vulnerabilities within the vulnerability management tracking list. Mitigated vulnerabilities should be reviewed on a quarterly basis to determine if more efficient mitigations may be deployed that could save time, maintenance expenses, or further reduce risk.

For patching or maintenance, any failed, disruptive, or unpatched systems become exceptions that become addressed as vulnerabilities under this policy. However, most failed or disruptive vulnerabilities will not remain exceptions. Failed or disruptive mitigations will be reworked and reintroduced into the vulnerability management process for resolution. On rare occasions, the combination of a low risk vulnerability and high cost of compensating controls may lead the organization to accept the risk of the specific vulnerability. These exceptions will need to be tracked and reported within the vulnerability list.

G. Vulnerability Management Reporting

All Reports of Vulnerability must be forwarded to the General Manager in the first instance. The time-line for internal Vulnerability reporting is within 24 hours of the incident and thereafter as follows (see Clause 6 for Reporting vulnerabilities or security issues by external parties):

In all cases the Company Data Controller will:

a) acknowledge receipt within 2 working days;

b) investigate the issue within a target time of 2 working days;

c) report findings, recommendations and conclusions back to the originator and the Company Management Team at the conclusion of b) above;

d) further action through to a satisfactory conclusion by all parties is reached;

e) take any further appropriate monitoring to ensure there is no repletion of the issue;

f) maintain records of a) to e) above.

The IT Department will issue monthly reports on patching and updating. The reports must include:

- Date(s) of last asset scan(s) and number of assets tracked
- The percent of systems actively tested for vulnerabilities and types of vulnerability scans and penetration tests used in the active testing
- The number of vulnerabilities detected in scanning
- The number of vulnerabilities remediated through mitigations classified by:
    - vulnerability risk
    - overall priority
    - time for resolution (in summary and in detail)
- The vulnerability scan or penetration test performed for each mitigation to verify proper implementation (note as pending if the testing is still in progress)
- The number of remaining vulnerabilities unmitigated
- Average time elapsed between vulnerability detection and mitigation by asset risk and value category
- The number of vulnerability exceptions added to the exception report
- The total number of vulnerabilities and mitigations within the vulnerability tracking list.

4. Audit Controls and Management

The Company directors and auditors may request documented procedures and evidence of the vulnerability management practice on demand. Examples of documented procedures and evidence include:

- Approved Maintenance Window Requests
- Approved Exception Lists
- Full or partial exports of the vulnerability management tracking list or system
- Full or partial copies of vulnerability scans and penetration tests conducted to discover vulnerabilities or to verify mitigations
- Vulnerability Management Reports

5. Enforcement

Employees found in intentional policy violation may be subject to disciplinary action, up to and including termination. The job performance of IT Department staff responsible for executing this policy will be evaluated based in part or in full on their ability to fulfil the expectations of this policy.

Regular inability of the IT Department to meet the requirements of this Vulnerability Management policy may be considered negligence and result in disciplinary action. Falsified reports or gross negligence in execution may be grounds for immediate termination or disciplinary action.

6. Reporting vulnerabilities or security issues by external parties

Should the need arise for an external party to report a perceived vulnerability or security issue from a device supplied by or rented from the Company then this should be sent in writing to:

The Data Controller
Innovation House
Envision Intelligent Solutions Limited
Silverwood Business Park
Craigavon
BT66 6SY

Or E-Mailed to: info@envision-is.co.uk

In all cases the Company Data Controller will:

a) acknowledge receipt within 2 working days;

b) investigate the issue within a target time of 2 working days;

c) report findings, recommendations and conclusions back to the originator and the Company Management Team at the conclusion of b) above;

d) further action through to a satisfactory conclusion by all parties is reached;

e) take any further appropriate monitoring to ensure there is no repletion of the issue;

f) maintain records of a) to e) above.

POL29 - Vulnerability Management Policy

7. Distribution

This policy is to be distributed to all Company personnel and IT Department staff responsible for Patch Management Policy support and management.

8. Policy Approval

Version 4.0

Description: Policy update

Signature

Approved By: _____ _____

[A signature by the Patch Management Authority acknowledges the requirements of the policy and becomes a de facto pledge to meet the requirements. A signature by the CEO or other executive acknowledges that the policy meets the needs of the organization. The executive that signs should be senior enough that their signature will compel other departments to comply with the policy.]

POL29 - Vulnerability Management Policy

Appendix 1

IT Resource Asset List

As per the Asset Management Policy, ISP006, the asset list of the Company covers all systems, software, firmware and devices of the Company. The asset list does not include devices outside of the control of the Company.

Examples of resources on the asset list include, but are not limited to:

- Network equipment
    - Firewalls (and installed software, firmware, security features that require updates)
    - Network switches (and installed software, firmware)
    - Routers (and installed software, firmware)
- Servers (websites, application hosts, virtualization platforms, etc.) and installed operating system
- Installed operating system, installed software, firmware
    - Workstations
    - Tablets
    - Laptops
    - Cellular devices
- Internet of Things (IoT) and installed software and firmware
    - Voice over Internet Protocol (VoIP)
    - Security Cameras
    - Wi-Fi Connected TVs
    - Wi-Fi Printers
    - Network Printers
    - Storage Area Networks (SAN)
    - Voice-activated devices (Amazon Alexa, etc.)
    - Door security badge-readers
- Operational Technology (OT) and Connected Infrastructure and installed software or firmware
    - Connected HVAC equipment

The asset list also includes:

- Type of asset (Server, PC, software, router, etc.)
- Device assigned owner (if a shared resource, the head of the associated department is the de facto assigned owner)
- Core OS, Firmware, or Software version
- Manual or automatic update?

- Updated by IT Department, automatic software update, third-party tool, or third-party service provider?
- Last updated
- Associated devices (i.e., for Adobe Acrobat software: installed on associated device: PC4362)

While the IT Department maintains responsibility for maintaining the asset list, department heads must inform the IT department about new assets (devices, installed software, etc.) deployed. Devices or software deployed without informing the IT department will be considered rogue devices and subject to blocking and removal.

The IT Department will conduct quarterly scans of the IT environment to verify that the asset list remains current and to detect rogue devices or software.