Vulnerability Management Policy

Version 1.2

Purpose

The purpose of this policy is to ensure a higher level of security for Koorliny Kaattijin’s IT Resources provided through vulnerability management.

Scope

This IT policy, and all policies referenced herein, shall apply to all staff of the organisation, client and other stakeholders, authorized guests, and independent contractors (the “User(s)” or “you”) who use, access, or otherwise employ, locally or remotely, Koorliny Kaattijin IT Resources, whether individually controlled, shared, stand-alone, or networked.

Policy Statement

- All patches or configuration changes must be deployed to Koorliny Kaattijin -owned or managed IT Resources per the timeframe stated in the Vulnerability Management Procedure.
- Information Security and Assurance (ISA) provides approved standard tools and methodologies for vulnerability assessments.
- All IT Resources must be part of a patch management cycle as defined in Patch Management Policy.
- Application and system owners are responsible for the assessment and remediation of IT Resources under their management or supervision.
- If a solution or remediation is not available to address a vulnerability, the ISA must approve any compensating or other mitigating controls.
- Application and system owners must have a written and auditable procedure addressing remediation steps.

Definitions

Compensating control is a data security measure that is designed to satisfy the requirement or some other security measure that is deemed too difficult or impractical to implement.

IT Resources include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

A patch is a software update comprised code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:

- Upgrading software
- Fixing a software bug
- Installing new drivers
- Addressing new security vulnerabilities
- Addressing software stability issues

Patch management cycle is a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. Patch management occurs regularly as per the Patch Management Procedure.

Remediation is an effort that resolves or mitigates a discovered vulnerability.

Vulnerability management is the practice of identifying, classifying, remediating, and mitigating vulnerabilities.

Related Policies and Procedures

Web Application Security Policy

Revision History

Version	Date	Description
1.0	01/23/2017	Initial policy
1.1	03/25/2019	Updated policy statement
	05/08/2020	Periodic Review
1.2	07/27/2021	Periodic Review

Policy Disclaimer Statement

Deviations from policies, procedures, or guidelines published and approved by Information Security and Assurance (ISA) may only be done cooperatively between ISA and the requesting entity with sufficient time to allow for appropriate risk analysis, documentation, and possible presentation to authorities.