Security Baselines Policy

Version number	6.2
Last Approved	Dec 18, 2025
Classification	PUBLIC

Overview

Applicability

The applicability of this statement falls under the purview of the Security Documentation Overview.

Purpose

The Security Baselines Policy defines minimally acceptable secure configuration standards applicable to all Company IT systems.

Scope

All Company IT-managed systems that store, process and transmit Company data are in scope.

Responsibilities

IT is generally responsible for applying the secure baseline configuration and ensuring that it is maintained and kept up to date. Where non-IT personnel may from time to time be assigned system owner/custodian responsibilities, this carries the additional responsibility of applying the secure baseline configuration and ensuring it is maintained and kept up to date.

System Configuration

A "Security Baseline" defines the minimum set of security related settings and configuration required by any Company service, device, or system at all times.

The design of the baseline build will depend on the hardware and/or service types and operating systems to be used. It should take into account security recommendations from the vendors or service providers, provided that the final configuration provides the required level of asset protection.

System Minimum Requirements

The following requirements apply to the baseline secure configuration, regardless of the hardware and software being used:

- Only approved, licensed and supported software installed
- Latest software updates, including but not limited to patches, hotfixes, service packs and firmware
- Malware protection with frequent updates, and real-time protection enabled
- Firewall enabled and configured to reduce the exposure of systems to network-based attacks
- No unnecessary or vulnerable services enabled, including unauthorised, or open file shares on user workstations
- Encryption for data at rest and in transit using industry current and supported encryption standards (e.g., AES-256, TLS 1.2)
- Encryption enabled by default for cloud systems and services (leveraging Company-managed keys where available and appropriate)
- The application of the principle of Least Privilege as the practice, allowing only enough access and permissions to perform the required work
- Standard IT and Security software and agents installed and enabled
- Web Application Firewall (WAF) required for all client facing SaaS production assets. Minimally acceptable rulesets include injection, URL sanitization, and traffic inspection.

Authentication and Authorisation

- Access to data, systems and services should be limited to authorised personnel only.
- Usernames must clearly identify the user they represent. For example, using a corporate email address as the username, etc.
- All applications that support Single sign-on (SSO) must have it enabled and enforced. Dual or social login options must be disabled for additional security.
- In the absence of SSO, MFA or other compensating controls are required for access to applications, systems and services that process Restricted data. See the Data Classification and Handling Policy for more details.

Document Control

Language	English	
Classification	Public	
Document owner	Aleksandr Zaldak	
Author(s)	Aleksandr Zaldak	
Approver(s) and approval date	Aleksandr Zaldak - IT Security Manager	Jun 19, 2025
Review cycle	Annual	
Next review date	Mar 6, 2026	

Version History

Date	Author(s)	Version	Changes
Dec 18, 2025	Art Machado, Angelina	6.2	Added Web Application Firewall requirements for client facing SaaS

	Kilmer		services
Jun 19, 2025	Aleksandr Zaldak	6.1	Full review of the policy. Language and content updated.
Mar 7, 2025	Aleksandr Zaldak	6.0	Annual review
Nov 1, 2024	Angelina Kilmer	5.3	Changed Policy classification from Confidential to Public
Mar 22, 2024	Aleksandr Zaldak, Art Machado	5.2	Full review of the policy. Language and content has been changed to ensure it meets the requirements of everyone within the scope of the policy.
Mar 3, 2023	Aleksandr Zaldak, Art Machado	5.1	Annual review; Updated TLS and OS Versions; changed formatting to ISMS styling + added to Confluence
Apr 22, 2022	Aleksandr Zaldak	5.0	Updated TLS and OS Versions
Apr 25, 2021	Roland Barber	4.9	Updated TLS and OS Versions