Security Baselines Policy

Version number	5.3
Last Approved	Mar 22, 2024
Classification	PUBLIC

Applicability

The applicability of this statement falls under the purview of the Security Documentation Overview (PF-ISMS-0000).

Purpose

The purpose of this document is to provide guidance on how IT systems should be configured. What software versions are allowed on the LTG network to maximize the protection of the confidentiality, integrity and availability of data processed. Besides the requirement of the system to be designed with security in mind right from the scratch, the subsequent related actions often involve (but are not limited to) the following:

- Configuration hardening.
- Presence of means for privilege separation.
- Periodically updating the underlying system software with the latest patches.
- Presence of system tools regularly performing security scans, integrity checks, backups etc.

Scope

All LTG IT systems that store, process and transmit LTG, its clients or partners data are in scope. This includes, but not limited to wired, wireless and mobile devices. Routers, switches, firewalls, servers and workstations. Bring your own devices (BYOD), when used to access any of the company information and its services, are in scope as well. QA and Test systems deployed in a segregated development/QA VLAN are exempt from this scope.

Responsibilities

- The **Information Security Manager** is responsible for implementing and maintaining the asset inventory for all Company owned systems.
- System owners are responsible for providing the information required and ensuring that it is maintained, corresponding configuration applied and kept up to date.
- Employees, contractors and partners that use BYOD devices are expected to align the configuration of their systems to meet these requirements. See the Bring Your Own Device (BYOD) policy for more information.

System Configuration

A "Security Baseline" defines a minimum set of security related settings and configuration which must be met by any given device, service or system at any moment of operation. The specifics of how the baseline build is designed will be dependent upon the hardware and operating systems to be used. Therefore, use specific guidance from service or vendor-specific advice, assuming that the resulting configuration offers at least the same level of asset protection.

System Minimum Requirements

Whichever hardware and software is being used, it is mandatory that the below are considered in the design of the baseline secure configuration:

- Systems must have all the latest software updates installed. This includes, but not limited to patches, hotfixes, service packs and firmwares updates.
- Malware protection software installed with frequent updates and periodic full (at least on a weekly basis) system scans enabled.
- Firewall enabled and configured to reduce the exposure of systems to network-based attacks.
- Laptops and portable devices have full-disk encryption enabled. BitLocker, FileVault and LUKS are supported options.
- No unauthorised, or open SMB shares on user workstations.
- The Least privilege as the practice, allowing only enough access and permissions to perform the required work.

Management Agents

For all **Company owned devices,** the following is mandatory during the provisioning:

- Inventory Patching agent
- Malware protection agent
- Privileged access management agent
- Mobile device policy manager
- DLP Agent (if applicable)

Supported Software

Only vendor supported OS and builds and installed applications are allowed on the LTG network and systems, including all BYOD devices.

Generic Service Setup, Usage and Provisioning

- Usernames must clearly identify the user they represent (for example: using a corporate email address as the username).
- MFA is required for access to applications, systems and services that process **Restricted** data. See Data Classification and Handling Policy for more details.

Network Related Configuration

The core network requirements:

- **All Office firewalls:** Must have “**Content filtering**” and “**AV/IDS scans**” enabled. Strict ACL applied and exclusions documented.
- **Encryption:**
  - Only industry recognized standards and cyphers to be used.
  - **Network service:**
    - **SSL/TLS** (1.2+) only. No Clear text authentication allowed
    - Medium Strength Cipher suite, B grade SSL as a minimum
    - SNMP v3+

    - **Wi-FI:** WPA2/WPA2 Enterprise with AES
    - **SSH/SSL key size -** RSA 2048+, SHA2
  - **Data at Rest Encryption - BitLocker + PIN, FileVault, LUKS,** Advanced Encryption Standard (**AES**) **256**
- **VPN:** Only authorised IKEv2/IPSec and SSL VPN services only. **PPTP is not supported**.
- **All WAN facing servers, including cloud hosted ones,** must have unnecessary services disabled, strict firewall rules and whitelisting enforced for all network, including management, traffic.

Specific System Configuration/Hardening

Secure configuration and hardening standards aligning with industry best practice must be applied to all corporate and BYOD devices accessing the LTG network.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview.

Document control

Language	English	
Classification	Confidential	
Document owner	@Aleksandr Zaldak	
Author(s)	@Aleksandr Zaldak	
Approver(s) and approval date	@Aleksandr Zaldak - IS Manager	Mar 22, 2024
Review cycle	Annual	
Next review date	Mar 22, 2025	

Change log

Date	Author(s)	Version	Changes
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