

METTLER TOLEDO Security Statement

1. Purpose and Scope

This document describes the Security practices that are in place for METTLER TOLEDO related to its corporate infrastructure and implementation processes. The statement does not address the specific controls around development and administration of the products that are developed and sold by METTLER TOLEDO.

2. State of the Art Practices

METTLER TOLEDO Corporate IT security measures are based on current state of the art IT best security practices as defined within the NIST Cyber Security Framework (CSF) and the International Organization for Standardization ISO27000 series. METTLER TOLEDO continues to improve its security practices beyond what is documented herein and has no obligation to notify customer/vendor of those changes. The information in the Security Statement is of general nature, irrespective of the specific METTLER TOLEDO system or service at stake. METTLER TOLEDO may provide further information relating to specific METTLER TOLEDO products or services in further product- or service-specific documentation. In case of conflict between the information in this Statement and any product- or service-specific documentation, the information in the product- or service-specific documentation will prevail.

3. Patch and Vulnerability Management

METTLER TOLEDO subscribes to patch notification services to receive notifications about regular as well as zero-day updates. The entire system and its components, i.e., including extensions and improvements, are assessed to identify vulnerabilities that can be eliminated. Whenever METTLER TOLEDO becomes aware of vulnerabilities (according to the CVE ratings), these are remediated in a timely manner.

In addition to operating systems, updates cover applications and network devices. Software obtained from 3rd parties are also included in the patch and update process.

4. Secure Basic Configuration

We have policies and procedures in place, aimed at ensuring:

- The scope of functions and thus the number of existing programs, software modules, services and network protocols of components are reduced to the minimum requirements for system operation.
- In principle, services not explicitly required are deactivated by default.
- In case a system is accessible to a larger group of users or has very critical functions, a granular role and authorization concept is enabled.
- Standard combinations of usernames and passwords are changed during the initial configuration. Where the built-in administrative account cannot be modified, it is disabled.

- By policy, each component and user has only the rights necessary to perform the intended actions. For example, applications and network services are not operated with administrator privileges, but only with the minimum necessary system rights (least privilege principle).

5. Encryption

We have policies and procedures in place, aimed at ensuring:

- Sensitive data (e.g., passwords or special categories of personal data) are stored or transmitted in encrypted form in the system.
- Only the usage of well-known, current, and secure cryptographic algorithms is permitted.
- Relevant cryptographic parameters are stored securely. Access to components is protected by secure authentication procedures, session timeouts, secured protocols, etc.

6. Authentication & Authorization

Many / Most applications support personalized identification and authentication. If this is the case, access is allowed to data and variables after successful authentication and authorization checks are completed.

We have policies and procedures in place, aimed at ensuring:

- Single sign-on is used for non-administrative access.
- Administrative access requires separate logon within the corporate network.
- Password strength and validity are managed.
- Multi-factor authentication is used for access to the corporate network.
- Hard coded usernames and password combinations are not used.
- Accounts not required for the operation of a system are removed or at least deactivated.
- A least privileged, role-based access strategy is used for provisioning.
- Segregation of duty risks are managed appropriately.
- Accounts are enabled/disabled in a timely manner.

7. Commitment to Absence of Malware and Spyware (Trustworthiness)

METTLER TOLEDO uses commercially reasonable efforts to ensure that its systems and applications do not contain malware, spyware, hidden code, undocumented backdoors, or other hidden functions (e.g., unauthorized forwarding of data) that could result in a compromise to the information security of the METTLER TOLEDO environment.

METTLER TOLEDO utilizes an endpoint protection system that is an advanced, comprehensive defense to perform threat detection using machine learning.

Mettler maintains a next-generation firewall (NGFW) which provides multi-layered advanced security and better visibility to protect the network and data center against advanced threats.

METTLER TOLEDO applies additional threat protections to help mitigate the risk of (D)DoS ([Distributed] Denial of Service) or other cyber-attacks.

8. Quality Assurance Process for Software

METTLER TOLEDO adheres to a standardized set of processes for secure software development with corresponding guidelines for secure coding, quality assurance measures and controls (such as peer group reviews, manual or automated source code reviews, external audits, OWASP Top 10 verification, etc.).

9. Security Tests

METTLER TOLEDO performs periodic penetration tests as well as both internal and external vulnerability scans to identify the potential risk related to attacks or other security issues. If vulnerabilities are identified within the scope of these checks, section Patch and Vulnerability Management is applicable.

10. Logging and Audit Trails

METTLER TOLEDO systems and applications are typically designed to log user interactions, security relevant actions, events, and errors in a format to allow ex post and central analysis. This data is exported and integrated into SIEM solutions for security event correlation by our Security Operations Center (SOC).

11. Physical Security

METTLER TOLEDO maintains and periodically tests a commercially customary disaster recovery plan that provides adequate system backup, technology replacement, and alternate (recovery) site capabilities in support of business continuity requirements.

METTLER TOLEDO maintains commercially customary physical security and access controls for its data center(s) and facilities.

12. Cyber Security Training

METTLER TOLEDO maintains a continuous security awareness and training program. Employees are provided anti-phishing and malware detection training on a regular basis. Additional phishing attempts are used to identify training gaps and areas that require remediation. Additional educational material and news articles are published on a continuous basis.

13. Data Retention

METTLER TOLEDO uses commercially reasonable efforts to ensure that all data is preserved in a manner that is appropriate for the type/source/classification of the data, prevents inappropriate disclosure, is retained only for as long as reasonably required, and is responsibly disposed of or destroyed in a manner that prevents content recovery.

14. Data Privacy

METTLER-TOLEDO has processes in place to comply with applicable data protection regulations. All details on our handling of personal data of customers and partners are set out in our privacy policy under www.mt.com/privacypolicy.

15. Cyber Security and Incident Response

METTLER TOLEDO maintains a 24x7 Security Operations Center to monitor and detect potential cyber security threats to the organization. Incident Response services are in place to support recovery and forensic requirements in case of a security breach. METTLER TOLEDO maintains use cases and playbooks that are required to respond to potential security events.

Disclaimer

The information provided herein is for your information only. It does not extend our liability in any way.

This information was prepared by using reasonable efforts and reflects METTLER TOLEDO's findings at the date of its creation. Without prejudice to any rights or obligations under existing written agreements, METTLER TOLEDO makes no representations, warranties, or assurances of any kind, expressed or implied, including but not limited to the accuracy, currency, completeness or reliability of the information provided. METTLER TOLEDO shall in no event be liable for any damages, including direct, consequential, incidental and special or any injury resulting from your access to or use of this information or from your reliance on any information provided.

The information contained herein is the property of and copyrighted by METTLER TOLEDO and may not be reproduced, disseminated, sold, distributed, published, circulated or commercially exploited without the express written permission of METTLER TOLEDO.

The scope of this document is limited to the scope of application of standard cyber security practices, i.e. to such group systems and applications falling under the ambit of NIST CSF and ISO27001 performed by Mettler-Toledo International Inc. METTLER TOLEDO has no obligation to adopt customer specified information security controls in order for that customer to be compliant with regulations applicable to their business. This document does not contain any statement relating to any local systems and application used by a METTLER TOLEDO group company and/or any METTLER TOLEDO product manufactured or distributed, or any statement, conclusion or indication relating to METTLER TOLEDO's compliance with any other or similar regulations and Customer, nor any other party, may rely on this statement for any such purpose.