



Our commitment to
information security

Protect IT

ThermoFisher
SCIENTIFIC

The systems and data being used to shape the future of science must be protected. Through our robust information security program, Thermo Fisher Scientific has developed a clearly defined set of information security policies and procedures that are designed to maintain the confidentiality, integrity, and availability of all data and systems within the company's environment. By protecting our data and the data of our customers, we can continue to support our mission to enable our customers to make the world healthier, cleaner, and safer.

The Corporate Information Security (CIS) department is comprised of a chief information security officer overseeing staff supporting the following areas:

- Program management and governance
- Security operations and technology
- Threat and vulnerability management
- Policy and compliance
- Risk management
- Security awareness
- Data protection and privacy



Protecting our people

Information security is the responsibility of every person working at Thermo Fisher; that's why we maintain a security awareness and training program designed to help all of our team members cultivate a "security first" mindset. All employees and contractors are required to review an acceptable use policy, as well as complete security awareness training on an annual basis. In addition, we conduct a variety of training events throughout the year—including phishing simulations and in-person training sessions focused on functional roles—which help our employees gain deeper understanding in specific areas of information security.



Protecting our data and systems

Thermo Fisher invests a significant amount of time and effort in developing and deploying secure platforms to meet the needs of our customers. We utilize a defense-in-depth approach to security, which ensures no protective mechanism is a single point of failure. Our protection systems are broken into several areas: network, infrastructure, data protection, and data center management.



Network protections

- Redundant firewalls
- Intrusion detection and prevention
- Distributed denial of service protection
- Web application firewalls for externally facing websites and applications

Server/client endpoint protection

- Antivirus/anti-malware
- Next-generation endpoint security for advanced threat detection, protection, and response
- Web content filtering for all employees and contractors
- Spam/malicious email blocking
- Continuous operating system patching
- Standard equipment configuration

Data protection

- Use of encryption for data at rest and data in transit where necessary
- Standardized processes for sanitization and destruction of assets
- Employees and contractors are granted access to systems and applications on a strict need-to-know basis to protect confidentiality, integrity, and availability of customer and internal data

Data Center management

- Maintain ISO 27001 certification for our North American Data Center
- 24/7 staffing with strict access control systems and procedures
- Full environmental management with redundant power backups

Secure processes and procedures

Information security is more than just installing the latest security tools or patching systems. Secure business processes and procedures are paramount to the security of our environment. Thermo Fisher maintains robust procedures in several key areas including: change management, data backup, and security incident management.



Change management

All changes to production systems, whether they are software, hardware, or network, are required to utilize a standardized change management process. The process is maintained within a change management system validated to 21 CFR Part 11 Electronic Document Management standards.

Data backup

Performing backups is an effective way to safeguard against the risk of losing data due to technical, human, or environmental factors. All critical systems are regularly backed up according to industry best practices based on the criticality and security requirements of the information involved. Backups are comprised of a combination of on-site, off-site, and cloud-based solutions providing a comprehensive backup strategy for our data.

Security incident management

100% prevention of security incidents is the ideal standard, but the reality of information security today is security incidents can occur due to new or unforeseen circumstances. Our fully staffed Security Operations Center continuously monitors our environment through a variety of automated and analyst-driven processes, resulting in quick detection and response to potential security incidents. Our security incident management processes include:

- Threat intelligence gathering and analysis
- Aggregation and analysis of system logs
- Emergency response management
- Email/phone support for reporting incidents
- Proactive threat hunting

Governance and monitoring

The information security program and its policies are aligned with the International Organization for Standardization (ISO) framework. Input has also been incorporated from the National Institute of Standards and Technology (NIST) Cybersecurity framework. Audits are conducted both internally and externally on an annual basis to ensure program adequacy.

Regulatory responsibility and program compliance

Thermo Fisher has information security compliance requirements that span several regulations, regions, and countries, and include the following:

- The Sarbanes-Oxley Act of 2002 (SOX)
- ISO 27001:2013
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Regulation (EU) 2016/679 of The European Parliament and of the Council (General Data Protection Regulation)
- Payment Card Industry (PCI) Data Security Standard, Version 3.2

ThermoFisher
SCIENTIFIC