



EFFECTIVE DATE: 07/16/2009

<i>Title:</i> IT Security Global Acceptable Use Policy	<i>Supersedes:</i> IT Security Acceptable Use Policy	<i>Total Pages:</i> 5
---	---	--------------------------

OVERVIEW:

Thermo Fisher Scientific strives to protect itself and its employees, affiliates, and business partners from illegal or damaging actions that may be performed by individuals knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Thermo Fisher Scientific employee, affiliate, and business partner that deals with information and/or information systems. It is the responsibility of every Thermo Fisher Scientific employee to know these guidelines, and to conduct their activities in accordance with all company policies and the Code of Business Conduct and Ethics.

Note: Employees who manage vendors and those who manage contracts (i.e. via vendor service agreements) with affiliates or business partners that access the global corporate network are responsible for ensuring their understanding and compliance with all IT Security policies.

PURPOSE:

This policy is intended to outline appropriate and inappropriate uses of Information Technology Systems, and to help protect Thermo Fisher Scientific employees, affiliates, business partners, and the company from inappropriate use of these systems.

SCOPE:

This policy applies to all Thermo Fisher Scientific employees, affiliates, and business partners that access the global corporate network. This includes all employees, contractors, consultants, temporary employees and personnel affiliated with third parties.

Individuals and organizations are expected to comply with this policy when performing any activity during the course of duties for Thermo Fisher Scientific, or when interacting with any Information Technology system or equipment owned or operated by Thermo Fisher Scientific, regardless of whether the interaction occurs during the course of Thermo Fisher Scientific duties or during coincidental use of these systems.

The listings of acceptable and unacceptable uses below are by no means intended to be exhaustive. Rather, these listings are intended to provide a framework to assist individuals in identifying acceptable or unacceptable uses for any system related to Thermo Fisher Scientific. Employees are expected to exercise good judgment with respect to their activities.

If you do not understand any provision within this policy please direct your questions to your management or contact the Global Information Risk and Security Management group via email at itsecurity@thermofisher.com.

POLICY:

Thermo Fisher Scientific systems and equipment are to be used for serving the interests and mission of the company, and of our clients and customers in the course of normal operations.

1. General Use and Ownership

- a. Users should be aware that the data they create and manage on the corporate systems remains the property of Thermo Fisher Scientific.
- b. Thermo Fisher Scientific may, in its sole discretion, block or limit Internet traffic that might negatively impact the network (i.e. hacking, malware, pornography, peer to peer, social networking and streaming media, etc.).
- c. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- d. Thermo Fisher Scientific has specific encryption requirements related to information that is deemed sensitive (confidential or secret such as PCI credit card or PII personal information), and recommends that any information that users deem sensitive also be encrypted. For guidelines on information classification, see Thermo Fisher Scientifics' Global Information Sensitivity & Classification Policy. For guidelines on encryption, see Thermo Fisher Scientifics' Global Encryption Policy.
- e. For various reasons including but not limited to security concerns, network maintenance purposes, troubleshooting, court orders, and/or requests made by Thermo Fisher Scientific HR or legal, authorized individuals within Thermo Fisher Scientific may monitor equipment, systems and network traffic at any time.
- f. Thermo Fisher Scientific may in its sole discretion audit networks and systems on a periodic basis to ensure compliance with this Policy as well as to ensure that all LAN/WAN/MAN's are configured in such a way as to protect the corporate flow of data from hacking attempts and those attempting to disrupt business.

2. Security and Proprietary Information

- a. The user interface (screen display, print media, etc) for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential determined by the type of data and/or the potential harm that could be caused if such data were made public. Examples of confidential information include but are not limited to: company private data, corporate strategies, PCI (credit card data), PII (Personally Identifiable Information), competitor sensitive data, trade secrets, specifications, customer lists, and research data, etc. Employees, affiliates and business partners with access, ownership or responsibility over such data should take all necessary steps to prevent unauthorized access to confidential information as defined in the Information Classification and Handling policy.

Here are some guidelines for protecting sensitive information:

- Label documents "Confidential," as appropriate
- Keep sensitive information in a locked cabinet or drawer
- Manage records following our Record Retention Schedule
- Never use a public Internet site (i.e. unprotected online storage) or an unprotected wireless network to post, store or send sensitive information
- Use corporate approved solutions for external sharing of sensitive information (i.e. encrypted email, encrypted USB or protected online storage)

Confidential information is any information that is sensitive and intended to be kept internal or protected. It includes things like new product designs, strategic business plans, and nonpublic financial information. It also includes personally identifiable information about customers or employees. The use and protection of personally identifiable information is subject to Company data privacy and security policies, as well as applicable privacy laws.

You must also be sure to safeguard confidential information that belongs to third parties, including our customers, suppliers, and distributors.

- b. Keep passwords secure, never divulge your password to anyone and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. All passwords must be strong passwords and changed in accordance with Thermo Fisher Scientifics' Global Password Policy.
- c. All company issued PCs, laptops, workstations and mobile computing devices (i.e. Smart Phones, BlackBerry, etc) must be secured with a PIN or password. For PC's a password protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Microsoft Windows users) when the equipment will be unattended.
- d. Encryption must be used in compliance with Thermo Fisher Scientifics' Encryption policy.
- e. Adequate protection against malware must be installed on computing resources and this protection must never be deactivated without express permission from IT Security. This implies up to date virus protection in accordance with the Global Anti-Virus Management policy and secure, up to date configuration of this software, including updates and security patches.
- f. Employees are prohibited from using his or her Thermo Fisher Scientific email address to post on social media, blogs or other online forums, unless the posting is made on behalf of the company.
- g. The installation or use of private/personal software or hardware in conjunction with Thermo Fisher Scientific equipment is not permitted (i.e. provided by 3rd parties such as USB sticks).
- h. Only Thermo Fisher Scientific approved (such as approved BYOD) or company provided devices may be connected to the corporate network due to the fact that it is impossible to know what potential malware or functions foreign hardware might inject.
- i. Employees must use extreme caution when opening e-mail attachments received from senders (known and unknown) which may contain viruses or other malware type malicious code. **(Internet links and executables should not be opened regardless of source)**. If there is any question as to how to handle an attachment, employees should contact the Enterprise Service Desk.

The activities noted in policy sections 3 and 4 are, in general, prohibited and are not exhaustive lists of prohibited behaviors. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Thermo Fisher Scientific authorized to engage in any activity that is illegal under local, state, federal or international law in the course of Thermo Fisher Scientific business, or while interacting with Thermo Fisher Scientific resources.

3. Unacceptable System and Network Activities

- a. Viewing pornographic or sexually explicit materials at work or via Company issued devices (including laptops) regardless of whether the viewing occurs on or off Company premises or during or after work hours.
- b. Excessive or unreasonable personal use of the internet during work hours.

- c. Infringement of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by Thermo Fisher Scientific.
- d. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Thermo Fisher Scientific or the end user does not have an active license is strictly prohibited.
- e. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- f. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, other malware, etc.).
- g. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- h. Making fraudulent offers of products, items, or services originating from any Thermo Fisher Scientific account.
- i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- j. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information.
- k. Port scanning or security scanning is expressly prohibited unless prior notification and authorization by Thermo Fisher Scientific is made.
- l. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- m. Circumventing user authentication or security of any host, network or account.
- n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
- o. Providing information about, or lists of, Thermo Fisher Scientific employees to parties outside Thermo Fisher Scientific.
- p. Using the System or Network in any way that violates company policies or the Code of Business Conduct and Ethics.

4. Unacceptable Email and Communications Activities

- a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Internal and External to customers or potential customers.
- b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages in addition to HR's harassment policy.
- c. Unauthorized use, or forging, of email header information.
- d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- e. Creating or forwarding 'chain letters', 'Ponzi' or other 'pyramid' schemes of any type.
- f. To prevent the unauthorized or inadvertent disclosure of sensitive company information, forwarding of company email is not permitted, such as auto forwarding to external addresses.
- g. Creating internal email addresses for external entities or auto forwarding email to external entities is not permitted without express approval from the Global IT Security Director.
- h. Use of unsolicited email originating from within Thermo Fisher Scientifics' networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Thermo Fisher Scientific or connected via Thermo Fisher Scientifics' network.

RESPONSIBILITIES:

- Each Global IT organization in Thermo Fisher Scientific has the responsibility to assist in the communication and implementation of this policy.
- A computer user or system administrator is responsible, upon suspecting a violation of this policy, to contact the Global IT Security group in writing or via a service desk request to report the incident.
- Report any loss of information, equipment and other security relevant items (i.e. loss of laptops, loss of keys and badges) immediately to the responsible unit or directly to your manager.
- Be aware of the fact that in case of the loss of a laptop or other mobile device, the actual value of the stored information might far exceed the value of the hardware itself.
- Immediately report any suspected incidents to your IT support group or directly to your manager.
- Immediately report any observed or suspected security weaknesses in information systems or threats to these systems to the responsible system manager.
- If after reviewing this policy you are unsure as to whether or not a specific action would be classified as acceptable or unacceptable, please inquire about the appropriateness of the activity with your immediate supervisor or manager.

ENFORCEMENT:

All Thermo Fisher Scientific employees, affiliates, and business partners are responsible for complying with this policy and the policies which are referenced by this policy. This includes all employees, contractors, consultants, temporary employees and personnel affiliated with third parties.

Any Thermo Fisher Scientific employees, affiliates, or business partners (including all employees, contractors, consultants, temporary employees and personnel affiliated with third parties) found to have violated this policy, or any policy referenced by this policy, may be subject to disciplinary action up to and including termination.

DOCUMENT HISTORY:

Version	Date	Author	Change Summary
1.0	05/19/2009	Thomas K. Watson – Director of Global Information Risk and Security	Baseline document
1.1	7/15/2009	Thomas K. Watson	Removed signature acknowledgement page
1.2	2/24/2011	Thomas K. Watson	Unacceptable use clarification (Section 3 a&b)
1.3	10/1/2013	Thomas K. Watson	General updates and guideline content