IT CODE OF CONDUCT

POLICY

nnit.com

TABLE OF CONTENTS

INTRODUCTION

The NNIT IT Code of Conduct applies to all NNIT employees, and external consultants working for NNIT.

Yearly retraining in the document is mandatory.

PURPOSE

In NNIT we are committed to follow the best practices for quality and security in order to safeguard information and systems belonging to NNIT and our customers. We wish to ensure the delivery of IT services in a safe and professional manner.

NNIT holds a number of certifications that allow us to deliver services to customers in the regulated industry. It is vital that we maintain these certificates through compliance with our policies and procedures.

The purpose of NNIT's quality and security requirements, including the NNIT IT Code of Conduct, is to ensure that we all are aware of our responsibilities and that we demonstrate a quality minded and secure behavior in our daily work with NNIT and customer systems.

It is crucial that all employees read, understand, and follow all relevant quality and security documents before work is commenced on any NNIT or customer system, application, infrastructure, or IT service delivery.

Thank you for keeping NNIT and our customers secure.

Signed,
Pär Fors, June 2021

Know what you need to know
Before you engage in any IT service delivery, whether internal or external, you must ensure that you are fully familiar with the requirements for the delivery.

The processes and procedures you need to follow are all described in cQPoint and your manager will assign the needed modules to you in the NNIT training system cQPoint.

Unauthorized, irrelevant, or private activities must not be performed on NNIT or customer IT environments.

When working on customer systems you must only perform agreed and work-related tasks.

Any misconduct can have adverse consequences for the relationship between NNIT and the customer and will be handled according to NNIT's warning and dismissal procedures.

There are a number of mandatory training sessions you must participate in before IT related work is commenced. Errors and incidents must not occur due to lack of training or failure to follow mandatory procedures as described in cQPoint.

If you experience that you are not competent to carry out your assignments, that you may require more training or that you do not quite understand the instructions, please let your manager know before you begin your assignment.

Roles and responsibilities
Working in a secure and compliant manner and delivering high quality IT services is a team effort and the correct handling and protection of our organization and customer's assets are everyone's duty. Every one of us must take personal responsibility for the quality and security of the information we own, provide, and work with.

Role	Responsibilities
All employees	Responsible for adhering to the NNIT information security requirements.
Quality & Security	Responsible for, and mandated to, setting the minimum security requirements, enforcing these and measure for compliance throughout NNIT at a global level
People Managers	Responsible for ensuring that employees are familiar with and work in compliance with NNIT's information security requirements and review on an on-going basis that this happens. They are further responsible for taking appropriate actions if there is evidence that the policy is not being adhered to.

CODE OF CONDUCT

Quality
In NNIT we have a high focus on quality in order to ensure that we meet the needs of our customers as well as applicable legal and regulatory requirements.

Within the regulated industry, such as the life sciences and financial sectors, the requirements for quality are high. Failure to comply with these requirements can have severe consequences for our customers and in some cases fatal consequences for end users – e.g. if a NNIT developed IT system supports the production of medicine, patients' health can be affected.
Information systems are a vital part of the quality value chain, as they control financial transactions, pharmaceutical controls, confidential personal data, etc. Therefore, following the procedures described in cQPoint are requirements both from our customers, our customer's auditors, and other regulatory authorities.

All Employees shall treat Material News confidential and may not disclose such information to any

Information Etchics
NNIT is an international company that endorses tolerance and respect between our employees. As NNIT employees, we are naturally expected to show ethical behavior in our daily work with colleagues,

business partners and other parties, and not use any information system for unethical activities, such as:

- Making offensive comments about race, religion, disabilities, and sexual orientation
- Supporting or initiating activities that are sexual, pornographic, political, or religious in nature
- Distributing messages that can be offensive or disruptive in nature such as chain mails, hate mails or similar
- Using NNIT systems or connections for work that is not related to NNIT's business e.g. work for a private company owned by an employee
- Working with IT systems under influence of e.g. alcohol or other substances
- Sharing copyrighted files (such as music or videos) with your colleagues

Awareness

The daily threats we face in a complex world of IT are numerous. They require constant awareness by all employees in order to avoid operational or security related incidents.

As an NNIT employee you play a significant role in order to secure the safety of NNIT information and assets. Your daily awareness of any actual or potential breach is therefore of paramount importance.

Many security breaches can be discovered or avoided by paying attention to your surroundings on a daily basis and ensuring that suspicious activity or missing controls are reported to the nearest management.

Example: Do you notice who is walking in behind you when you are opening a door, does the person have an ID card? Do you recognize him or her? Have you heard or seen something suspicious? In these instances, you must notify the appropriate colleagues.

When travelling

When travelling, you are outside the secure locations of NNIT. You must therefore always take extra care to protect NNIT's information and assets. Always ensure that you keep a close watch on your laptop, smartphone, and documents as these are easily lost or stolen.

Using Screen filters

If you use your laptop computer in crowded areas, such as airports, trains or planes, people can read over your shoulder and potentially see restricted information. To avoid this, please ensure you install a screen filter on your laptop. A screen filter makes it very difficult for others to read what is on your screen.

Speaking in public

Please be aware of what you say in public areas such as canteen areas, taxis, trains, and other areas where non NNIT employees can be present. Never loudly discuss NNIT or customer matters in such areas either directly or via phone.

Mobile Devices

Mobiles devices are easily lost or stolen. As today's smartphones can contain a large amount of classified data – such as e-mail, documents, etc. – it is important that they are protected and kept under close observation.

All mobile devices must be protected by using a PIN code or password which is enforced centrally. It is not allowed to bypass these security controls in any way. Pin codes and passwords can be substituted with fingerprints, face recognition or other biometrics.

If you lose your phone, please contact the NNIT Service Desk immediately for disabling the device.

It is not allowed to store NNIT data on personal devices that are not centrally managed and secured.

Our Office Environment
You are the primary responsible for the assets and data entrusted to you. Information assets include, but are not limited to, documents, data, services, systems, software, hardware, and know-how. It is essential that you work with due care and attention to ensure that these information assets are protected in your daily work.

Clear Desk Policy
In NNIT we have a 'clear desk' policy. This means that you must remove all confidential information from your desk when you leave your desk. All papers and storage media (such as USB keys, CD's, etc.) containing confidential NNIT data, must be locked in cabinets and drawers to reduce the risk of unauthorized information disclosure. Laptop computers must also be safely stowed away each day to minimize the risk of theft.

Lock your Computer
When leaving your computer unattended, always remember to lock it to prevent unauthorized access to information. This can be done quickly by pressing the "Windows Key + L" simultaneously.

Teleworking
We cannot secure and control your privately-owned equipment, hence it not allowed to work with NNIT documents, spread sheets etc. and to transfer files to and from NNIT and home equipment (via mail, USB, etc.) as this introduces the risk of data leakage and potential virus outbreaks. The only safe access to NNIT resources from non NNIT equipment is by using the Citrix solution or our remote outlook service. They are specifically designed to be used on home equipment.

Your NNIT computer or smart phone is strictly for your personal use and you must not share with anyone e.g. spouse, children, or friends.

Classification
In order to protect NNIT and customer information in the correct way you need to pay close attention to the classification of the data you are handling on a daily basis. In NNIT we operate with five levels of classification:

- PUBLIC
- INTERNAL USE
- RESTRICTED COLLABORATION
- RESTRICTED INTERNAL
- CONFIDENTIAL

Public: Non-sensitive or open information that can be freely released to anyone such as product brochures and public websites.

Internal use: All internal data meant for NNIT eyes only or a specified audience such as customers or partners.

Restricted Collaboration: Data used in digital collaboration with customers, partners, suppliers, and group compagnies

Restricted Internal: All sensitive internal data that should not be distributed outside NNIT, including design documentation for NNIT-systems, geo-restricted data, non-sensitive personal data, employment contracts etc.

Confidential: Restricted information with a limited audience such as Business-sensitive data, customer contracts, bids, merger and acquisition documents, sensitive personal information, etc.

Internal and confidential information must be treated with the highest care

Printing
For both confidentiality as well as environmental reasons, please keep printing to a minimum and consider if text can be read on screen instead.

Printed material may contain restricted information and must never be placed in office waste baskets. Please ensure that you all such documents are disposed of either in the special containers meant for classified documents or by using a paper shredder.

Storing Information
To safeguard against data loss, you should try to avoid using local storage media, e.g. the hard drive on your laptop. To ensure a proper backup of your data, you must store your data on network drives or drives with network synchronization enabled.
Final versions must always be stored on the appropriate company storage, such as department file shares, SharePoint sites etc.

Encrypting Data
Information on laptops, USB sticks, etc. can be relatively easy to read if devices are lost or stolen.

All internal or confidential information placed on such devices should be encrypted in order to ensure that restricted data cannot be read by unauthorized individuals.

Unencrypted storage of confidential information on USB memory sticks, DVDs or other removable media is not allowed.

You must keep the amount of NNIT data stored on local storage media to a minimum.

External Storage
NNIT uses Microsoft OneDrive for Business as a supplement to the Home Drive on your computer. OneDrive for Business can be used for internal file sharing and collaboration.

The use of alternative external storage providers such as Dropbox, Google Drive, Microsoft OneDrive Personal, etc. for NNIT information are strictly prohibited as NNIT have no control of how this data is used or stored once it has left NNIT jurisdiction.

Your identity
When using NNIT systems, your system credentials are unique and must never be used by anyone other than you. Shared user IDs and passwords are only allowed on systems that do not support the use of multiple user accounts. If share user ID's are used, a manual activity and change log must be recorded.

Passwords and PIN codes
If you suspect that your password has been disclosed, please contact Service Desk immediately for a password change.

Passwords are strictly personal and must not be written down or stored in non-secure places such as clear text files on your computer or network shares where other people can gain access to them.

Passwords are required to have a certain complexity, which is electronically enforced.
Avoid combinations that are easy to guess such as your name, children's names, popular movies, etc.
Choose a password that is easy to remember and doesn't make sense to anyone else than you.
Passwords used for NNIT computer systems must not be reused for non-NNIT computer systems or reused on multiple internal NNIT systems at the same time.

Never reveal personal details such as passwords or PIN codes via phone or e-mail. Not even to the Service Desk which has other methods to assist you, that do not require your credentials.

Hardware
In NNIT we do what we can to secure our IT equipment for your safety. However, we cannot guarantee the security of equipment not belonging to NNIT.

Example: A computer virus on a personal USB key can quickly spread throughout NNIT networks with potentially disastrous consequences. For this reason, only NNIT equipment is allowed to be used in your daily work. You are consequently not allowed to connect personal owned equipment (such as USB keys, smart phones or computers) to NNIT equipment or networks, nor is it allowed to place unauthorized wireless access points in NNIT premises or connected to NNIT networks.

The office environment is only made for office equipment. It is not equipped nor secured for hosting servers or other production or test equipment.

Software
Untested software can introduce vulnerabilities to computer systems and networks. It is therefore important that all software in use within NNIT is tested and approved. Use of unlicensed or pirated software is naturally strictly prohibited.

Some software is dangerous to use on a corporate network. Therefore, any unauthorized tools made for the purpose of system hacking, password guessing, cracking, vulnerability scanning, etc. are not allowed.

To reduce the risks against our infrastructure, NNIT frequently monitor the installed applications on all computers and reserve the right to block and remove any unauthorized software that can be seen as a potential risk or software with no clear business justification.

The download and use of software for private use is not allowed.

Using E-mail
NNIT systems should only be used for private purposes to a limited degree. Private use of the e-mail system shall be indicated expressly in the subject field by using the word "private".

Caution should be taken when opening mails and/or attachments from unknown senders. They can contain malicious content such as computer virus code or fraudulent messages, etc. As a general rule, only open plausible attachments from trusted senders. If in doubt, contact the sender prior to opening the mail/attachment.

Internal or confidential NNIT data must only be sent to approved partners, suppliers, customers or other third parties that have signed a non-disclosure agreement. This is crucial to ensure that NNIT information does not fall into the wrong hands.

Web based e-mail is allowed for private purposes using NNIT computers (e.g. Gmail, Hotmail, etc.). However, in order to prevent viruses or similar to NNIT networks and preserve confidentiality, you must not upload or download attachments from such webmail services to NNIT computers. Nor must you use web-based e-mail to submit any data or attachments belonging to NNIT. It is not allowed to automatically forward private e-mails to an NNIT account or vice versa.

You must not share your NNIT e-mail address on publicly available websites, unless it is required by business.

Instant Messaging

Instant messaging clients can introduce security issues. Therefore, only approved NNIT instant messaging clients are to be used, as they are designed to protect you and our infrastructure.

Communication using instant messaging has the same legal validity as e-mail and other written communication and is therefore logged. Please keep this in mind when communicating in this way.

Browsing the Internet

A high number of threats, such as virus and malware, are present on the Internet. Known websites, that contain a risk of malicious content or contain material that can be considered offensive, illegal or in any other way be harmful to NNIT standards and infrastructure, will be blocked.

Show caution when using the Internet, as many sites exist solely to trick visitors in order to steal information or money from them.

A good rule to follow on the Internet is: If something seems too good to be true, it usually is. Good browsing practice is to not follow untrusted links and stick to business related sites.

As with e-mail, using the Internet to share files belonging to NNIT, containing NNIT data, must only happen to approved partners, customers or other third parties that have signed a non-disclosure agreement.

Using Social Media

The use of social media (such as Facebook, Twitter, or LinkedIn) from NNIT computer systems must not interfere with our main business tasks.

Social media must not be used to distribute internal or confidential NNIT information. When sharing pictures, you should be aware not to show any restricted information. You should e.g. never show pictures of NNIT ID cards, computer screens, etc.
If you are visiting Facebook, Twitter, etc. this is conducted in a private capacity and all communication, opinions and statements should reflect this.

Official statements regarding NNIT must be coordinated with NNIT Communication. It is also a good idea to consult NNIT's Social Media & Blogging guideline before using any social media. Find the guideline on Communications' site on FaceIT.

Computer Viruses

You must not attempt to remove malware without expert assistance, as malware is often complex and sophisticated. If you suspect infection by a malware, you must immediately power down the computer involved, and contact the local IT department or Service Desk.

Once a computer system is cleaned or replaced after a malware incident, all impacted users must change their passwords.

The largest risk of computer viruses comes from browsing untrusted websites, clicking links, and opening attachments to e-mail. However, some viruses (or 'worms') can also spread without your interaction by using vulnerabilities in software and operating systems. For this reason, you must always ensure your software is updated, and you must not install unapproved or personal software as this can introduce virus code and makes patching vulnerable software difficult.

Using tools and services on the Internet.
Using free tools and services on the Internet can only be done by strictly observing the restrictions set forth in Procedure for Handling of Classified Documents. The terms and conditions covering these tools and services normally stipulates that the tool provider obtains the full rights to use, sell, rent out etc. to the information/material uploaded to the tool. The result of this is, that you must sanitize the information to a level, where it can be classified as "Public" prior to the upload.

Security Controls
NNIT will always aim at implementing security controls that minimizes the impact on and annoyance for end users. However, the implemented security controls are there to protect our infrastructure and you must not interfere with them by e.g. disabling anti-virus controls, circumventing passwords, or PIN code controls, or in other ways weaken any controls on any system or device in NNIT.

If a security control prohibits you from doing your work, please contact Q&S Security.

Correspondence and other means of communication using NNIT systems including e-mail systems are considered written correspondence that, to the extent permitted by law, belongs to NNIT. NNIT can therefore have disposal of any type of correspondence to and from the company. To the extent permitted by law, any correspondence to and from the company's workplaces may be extracted and presented in legal actions involving NNIT. To the extent permitted by law, NNIT reserves the right to continuously monitor the use of NNIT IT systems.

NNIT only has access to private correspondence as part of the general operational monitoring, including the occasional control of the system load, etc. to and from each employee's workplace and in any event only to the extent permitted by law. Compliance monitoring will also enable NNIT to hold employees accountable in case of proven violation of the NNIT IT Code of Conduct.

About NNIT

NNIT is a leading provider of IT solutions to life sciences internationally, and to the public and enterprise sectors in Denmark. We focus on high complexity industries and thrive in environments where regulatory demands and complexity are high.

NNIT consists of group company NNIT A/S and subsidiaries SCALES, Excellis Health Solutions and SL Controls. Together, these companies employ more than 1,700 people in Europe, Asia and USA.

nnitcontact@nnit.com