CYBER SECURITY INSTRUCTIONS AND BEST PRACTICES

- When working in Wärtsilä premises
- When working at customer sites
- When working in supplier/sub-contractor premises
- When working at home
- When travelling

ENERGY
ENVIRONMENT
ECONOMY

WÄRTSILÄ

CYBER SECURITY INSTRUCTIONS AND BEST PRACTICES

This booklet presents a brief overview of cyber security instructions and best practices. It is distributed to all Wärtsilä employees and suppliers.

Cyber security is protection of assets in cyberspace from cyber attacks. Cyber security means Wärtsilä's ability to secure its people, information, systems and reputation in cyberspace. Cyberspace is the always-on, technologically interconnected world; it consists of people, organisations, information and technology.

Cyber security in Wärtsilä includes risk management in both our internal operations (IT systems, factories, logistic centres, etc.) and external operations (Wärtsilä products and services).

More information is available on
Compass → Our Wärtsilä → Wärtsilä Wiki → Cyber Security

Wärtsilä digital information

Digital information is valuable to Wärtsilä. You create, evaluate and use digital information, and make decisions based on it (e.g. e-mails, electronic documents, web pages).

Cyberspace risks also arise from digital information.

What should you do with digital Wärtsilä information?

- Share only the information recipients need or have a valid business reason for.
- Label sensitive information. For example, at the beginning of an e-mail indicate: "Sensitivity: confidential".
- Print and copy only when necessary – extra copies increase the risk of information falling into the wrong hands.
- Store digital information on USB memory sticks only when necessary.
- Store master copies of your most valuable items in Wärtsilä systems – e.g. IDM, Compass.
- Report any abnormal digital information sharing to the Wärtsilä Global Helpdesk.

Wärtsilä product security

Internet connected industrial products enable Wärtsilä to help customers enhance their business. However, it will also introduce numerous security concerns. Operations using industrial internet connections need to be secured, not only from unintentional human mistakes but also from intentional malicious acts. Wärtsilä's product security area is tackling these issues.

More information is available on
Compass → Our Wärtsilä → Security → Automation

Access rights and passwords

All access rights and passwords are personal to you and connected to your identity.

- You must not disclose your access rights or passwords to anyone.
- Since a password equals proof of identity, protect your identity by choosing only strong passwords (non-guessable and meaningless strings of characters).
- Nobody has the right to ask you to reveal your password. You should report any such instances to the Wärtsilä Global Helpdesk.
- Access rights apply also to buildings and premises. Don't let people enter protected areas without the correct authorisation.
- If you suspect that your password has been leaked, change password for each resource it is used and do not use that same password in the future.
- Never use the same password for Wärtsilä corporate resources as you do for private purpose resources.

More information is available on
Compass → Our Wärtsilä → Security → Information Security

Computers, software, equipment and network components

All digital devices, equipment, software, applications, and Corporate IT resources provided by Wärtsilä are meant for business use. Installations and updates must be made by authorised persons with a proper work order issued by an authorised party – typically by the Wärtsilä Global Helpdesk on an order from your superior.

- You are not allowed to install unlicensed or unauthorised software or applications. Wärtsilä may have to pay penalties for unlicensed or unauthorized components.
- You are not allowed to store unlicensed material or unauthorised copies of copyrighted material (e.g. music and movies).

Mobile phones and tablets

Mobile phones, tablets, and mobile phone subscriptions provided by Wärtsilä are for business purposes. The holders are solely responsible for the protection of these mobile phones and tablets.

- Your device(s) must be protected by a PIN code. See the manual of your device on how to set the PIN code for you device. This is particularly important when you are using your own device for business purposes.

- When processing and storing classified Wärtsilä information in your device, the same rules apply as when using a SONAD computer.
- If you need to use wireless services (Wireless LAN, Bluetooth, etc.), connections should be made to known and trusted devices and networks only. Please turn off any wireless services you don't need.
- Applications to devices must be installed from certified and trusted application stores (e.g. Apple App Store, Google Play, Windows Phone Marketplace).

Internet, social media and e-mail

It is important to distinguish between business use and private use of the internet, social media (e.g. Facebook, LinkedIn, Twitter) and e-mails. Keep in mind that when you use the internet with a Wärtsilä provided device, you are representing Wärtsilä too.

- Use Wärtsilä networks for business purposes mainly. Whilst private use of the internet and social media is allowed, retain the same code-of-conduct as with Wärtsilä business communications.
- Do not share business information privately on the internet (e.g. discussion forums or private social networks).
- Upload and share Wärtsilä digital information to public services (e.g. Facebook, LinkedIn, Twitter) with consent from your superior and Communications.
- Use Wärtsilä managed mailboxes (@wartsila.com) for business purposes. Do not use private e-mail accounts for sending or receiving business e-mails.
- Your company e-mail is for business communication, and private e-mail is for private communication.
- Avoid clicking web links in suspicious e-mails. Report suspicious e-mails to the Wärtsilä Global Helpdesk for further analysis if needed.

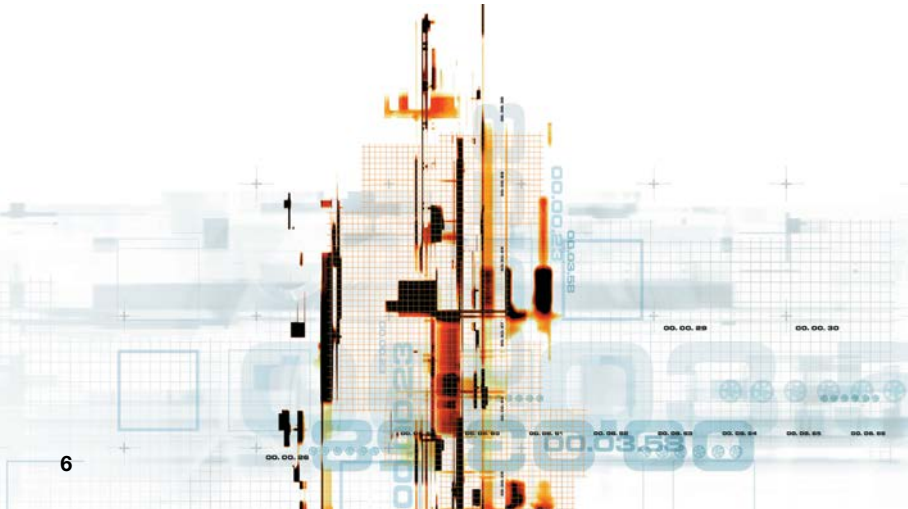
Malware and phishing

Viruses, Trojan horses and Worms are examples of malicious software – known as malware – intended to harm the computing environment or, in some cases, to spy on the user.

Phishing is about tricking internet users into revealing sensitive information about themselves (e.g. usernames, passwords or credit card numbers).

Wärtsilä computers are equipped with malware protection, intrusion detection and applications. However, you still need to take precautions:

- Don't open any e-mail attachments when the e-mail content is unfamiliar or illogical, or if the sender is unknown to you.
- Be suspicious of e-mails asking you to visit a web site you don't know. It may be an attempt to steal Wärtsilä's information and to install malware on your computer.
- Wärtsilä Corporate IT support will not install software or updates to your computer without your consent. If you receive such a request, report it to the Wärtsilä Global Helpdesk.
- Contact the Wärtsilä Global Helpdesk always if you have – or suspect that you have – malware on your computer. This will prevent larger scale damage from happening.
- When you have business tasks with Wärtsilä third parties or customers and they suspect that Wärtsilä might have security problems, instruct these third parties and customers to report security issues to Wärtsilä at www.wartsila.com/en/security.



Common sense and precautions

You may be tricked into answering questions and revealing sensitive information. Such requests may be done by phone, via e-mail or, for instance, by asking you to fill in a questionnaire. If you are unsure, ask for what purpose such Wärtsilä information is requested.

Internet connections leave traces and opened files will be stored locally in devices you use. Remove your traces if you have used public computers by, for example, clearing web browser cache and deleting downloaded files from local disks.

Leaving USB sticks, CD-ROMs, or other storage devices intentionally in public places is a means for tricking users to bring malware into Wärtsilä's internal systems. If you find such devices, and you don't know their origin – do not open them with your Wärtsilä device.

Consider Wärtsilä cyberspace risks in the same way as you consider your personal information risks on the internet!

Reporting

It is your duty to report cyber security issues.

- If you suspect that there may be a cyber security issue(s), please contact the Wärtsilä Global Helpdesk immediately. Fast reaction is important with cyber security issues!
- Always report lost or stolen Wärtsilä equipment to the Wärtsilä Global Helpdesk.
- If you suspect that cyber security has been breached at Wärtsilä customer installations, contact Technical Services at SiteSecurity@wartsila.com.

DO's and DON'Ts for Wärtsilä cyber security

Wärtsilä's digital information is valuable! Always keep these Wärtsilä cyber security instructions and guidelines in mind.

- Back up your business information regularly. In the event that the backup is on external media, remember to encrypt it and keep it in a locked and secure place.
- Share – don't store: make sure the information you possess is not stored on your computer only.
- Don't take your laptop or other devices containing Wärtsilä information with you if you don't need them.
- Don't leave your bags, computers or other devices unattended.
- Always report any incident or suspicious situation.
- If you don't know what to do, contact the Wärtsilä Global Helpdesk.

WÄRTSILÄ