Uhrenholt Information Security Policy

Prepared by: Lars Filstrup, VP, IT

Approved by: Klaus Vestergaard, CFO

Date: August 24, 2022

Version 1.0
Date: August 24, 2022

Table of Contents

Purpose 3

You are always responsible for what happens on your company IT-devices 3

Handling of confidential or personal (*) data 4

Security against computer virus – antivirus program 4

Internet, email, and calendar usage 4

Unacceptable use of the internet by employees includes, but is not limited to: 5

Backup 7

Wireless network and VPN 7

Purchasing of IT-equipment & Phones 7

Contacting IT Support 7

Purpose

The confidentiality, integrity, and availability of information, in all its forms, are critical to the on-going functioning and good governance of Uhrenholt.

In our daily work, we are all very dependent on the IT-systems holding this information, and consequently it's crucial that our IT-systems are available, secure, well-performing, and used according to the rules defined by the management.

Group IT is constantly maintaining and extending Uhrenholt's security tools, to protect our IT systems from computer viruses, spam, malware, hackers, and other external threats.

In this document we outline the rules and procedures that all internal employees in Uhrenholt must respect, all with the purpose of securing and protecting the information assets of Uhrenholt.

It is your responsibility to read, understand and follow the guidelines and use our IT-systems within these rules/policies/procedures.

Failure to comply with the rules and procedures mentioned in this policy will be considered a serious violation and may have consequences for your employment.

You are always responsible for what happens on your company IT-devices

You are not allowed to leave your company IT-devices (computer, tablet, cell phone) to anyone not authorized to have access to the computer systems at Uhrenholt. When leaving your computer, you should always lock the computer.

The installation of any kind of software is strictly prohibited unless it's software available in Uhrenholt Software Center or otherwise agreed with IT Support.

In your everyday you must make sure no one else has the knowledge of your passwords as in case of misuse it will be you who will be held responsible.

Employees who have cell phones or tablets (private or company owned) that are synchronized with the email server at Uhrenholt must have an access code on their device. The code must be at least 4 digits. It is 100% your responsibility to secure that this happens accordingly.

The data of the company is the property of the company and must be looked upon as such. It is therefore not allowed to copy these data to non-company IT-devices, eg. your private computer, USB-stick, tablet, cell phone or private subscriptions of cloud services like Dropbox or Google drive. It's okay to copy company data to official Uhrenholt USB-sticks, eg. for sharing a corporate presentation on a meeting, seminar etc.

In general, please be very careful using only company USB-sticks you have received from IT Support or a person you trust.

It's your responsibility to contact IT Support immediately should one of your company devices be stolen or lost.

Handling of confidential or personal (*) data

Always make sure that confidential data and personal data is saved in the right folders on the right data drives, where only people with the correct permissions can access it. E.g. department specific data in folders on the G-drive and personal date in folders on the P-drive. Never save confidential/personal data on open common data locations like the T-drive, as data on these locations might be open for all Uhrenholt employees, and never save personal data in emails.

As an IT user you often print documents, notes, or other material alike. These documents can be confidential and should be handled with the right care. You are responsible for confidential/personal printouts so that they do not end up in the wrong hands. You should always, right after having printed this type of materials, make sure to remove these documents from the printer/copier.

*) Personal data: Data protected according to GDPR or other personal data protection regulations

Security against computer virus – antivirus program

All servers and computers are installed with an antivirus program. This program is updated automatically.

To minimize the risk of virus on your computer you must follow these guidelines:

1) Piracy software and/or unauthorized copies are not, under any circumstances, allowed to be used.
2) Do not download, install, or open any unknown programs or anything alike from emails (filename usually ends on EXE)
3) Do not click on any links in emails unless the email is from a trusted colleague/partner, and even then, pay attention if anything looks suspicious. If you are in doubt about the validity of an email, please always reach out to IT Support for help.
4) Do not connect USB sticks or other similar devices to your computer unless you receive it from a trusted partner/supplier.

You should not be embarrassed if you get a virus on your computer, so please report any incident to the IT Support immediately. The sooner IT Support knows about it, the better, as it will limit the damage.

Internet, email, and calendar usage

- Uhrenholt employees are expected to use the Internet responsibly and productively. Internet access is primarily for job-related activities and personal use should be limited.
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.
- All Internet data that is composed, transmitted and/or received by Uhrenholt computer systems is considered to belong to Uhrenholt and is recognized as part of its official data.
- Under certain conditions, Uhrenholt is entitled to check the contents of emails, employees' use of the Internet and the content of laptops, cell phones and tablets which belong to Uhrenholt. This is no regular practice but can be put in effect e.g. in case of specific indication for unlawful or otherwise abusive usage of such components (e.g. when company IP is exposed to third parties).

Such investigations will be limited to what is necessary to clarify such issues and proportionate in relation to the relevant occasion. If you mark folders, files or emails as "PRIVATE" on your own network drive (C: / P: / OneDrive) or in Outlook, these will be respected as being private, and Uhrenholt will not check respective contents – unless it has specific indication that such classification has been made in an abusive manner, i.e. to hide company related conversations or other files. You are not allowed to mark any company related conversations, files or other material as being PRIVATE.

- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, but is not restricted to, the use of vulgar or harassing language/images etc.
- All sites and downloads may be monitored and/or blocked by Uhrenholt if they are deemed to be harmful and/or not productive to business.
- Uhrenholt wishes to promote transparency and openness and we all have a calendar in outlook. You must use your calendar actively which means that if you are on holiday, participate in seminars, are in a meeting or otherwise engaged, it is clearly stated in your calendar. This way your colleagues do not have to waste time on calling/mailing you if you are not there.
- When you are absent you must make sure that your auto response is activated with an alternative point of contact during holiday, illness, training etc.
- It's absolutely prohibited to use private email accounts for work purposes, including forwarding business emails to personal private accounts or other external email accounts.

Unacceptable use of the internet by employees includes, but is not limited to:

- Access to sites that contain obscene, hateful, pornographic, unlawful, violent, or otherwise illegal material.
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Uhrenholt email service
- Stealing, using, or disclosing someone else's password without authorization.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the organization.
- Introducing malicious software onto the company network and/or jeopardizing the security of the organizations electronic communications systems.

If an employee is uncertain about what constitutes as acceptable Internet usage, then he/she should ask IT Support for further guidance and clarification.

Password policy:

To prevent others from abusing your user account, it's important to have a secure password.

- **Selecting an acceptable password:**

  It's a good idea to choose a complex password, but also a password that is easy to remember, e.g. a sentence like "ilovethe6guysinIT!", "mycuteDog_has4legs", …

  You are unable to choose a password which is identical to any of your 12 previous passwords.

- **Storing passwords:**
  Passwords must never be stored electronically in clear text or on a piece of paper next to the computer

- **Password length:**
  Passwords must be at least 12 characters.

- **Passwords must NOT contain:**
  - Users account name
  - Part of user's full name
  - The Emborg name
  - The Uhrenholt name
  - Consecutive figures
  - Common sequences (like qwerty)

- **Requirements for password content**
  Passwords must contain characters from at least three of the following four categories:

  - Capital letters (A - Z),
  - Small letters (a - z),
  - Basic 10 digits (0 - 9)
  - Non-alphabetic signs (for instance: !, $, #, %).

  Complexity is maintained when passwords are changed or created.

- **Days between forced change of password**
  Every 3 months you will be asked to change your password, unless your password is a minimum of 18 characters, in which case it is every 6 months

- **Use of autologin features**
  Facilities for automated logins (such as scripts assigned to keys or clear text passwords embedded in programs) must not be used.

- **Passwords are strictly personal**
  Passwords are strictly personal and may not be shared with others.

Backup

All our servers are backed up daily according to our backup procedures. You must be aware that the local drives (typically the C and D drive) on your laptop are not included in this back-up. Consequently, it's your responsibility that no data is saved only on your local desktop/laptop.

Wireless network and VPN

The Wireless **Guest** network is to be used by guests of the house. For safety reasons we wish to keep our internal networks (cabled and wireless) and the guest network separated. For the same reason the guest network only has access to the internet and not to the company network. To set the record straight it must be emphasized that guests are **not** allowed to connect their computers via cable as they then will have access to the company network. It's the hosts responsibility to ensure that these rules are respected.

Due to security reasons, we do not want any kind of mobile devices or private devices (laptops, tablets, mobile phones) on our company networks (cabled or wireless). If you want to connect your mobile phone or any kind of private devices to our network, then please use the Wireless Guest network (if available).

If you need any kind of access from your laptop when out of office, then either use a local wireless network (if available) or setup your mobile phone as a hotspot and establish VPN connection on your laptop.

Installing the Cisco AnyConnect VPN or any other VPN software/tunnel on a **private device** such as Phone, Desktop or Laptop, and using it to connect to the UH network is **strictly forbidden** and could potentially compromise Uhrenholt!

Purchasing of IT-equipment & Phones

If you need to order any hardware or software (not already available in the Software Center), you do so by contacting IT Support via email.

Ordering of new IT-equipment must always be approved by your manager.

The installation of software must also be done in agreement with IT Support.

Contacting IT Support

Business Critical IT Support can be reached on +45 64 212 105 (during Danish business hours).

All other kind of IT Support Inquiries should be sent to it@uhrenholt.com

Please be as accurate as possible when you report a problem to IT Support, as it makes debugging faster and thus saves time for the IT Supporters and yourself.

You can search and find the IT Support email address and support number in Outlook.