HFBK
Hamburg

Information Security Policy of the HFBK Hamburg

The Executive Committee of the HFBK Hamburg has approved the following policy:

1
Background, purpose and application

Universities face particular challenges in regard to information security, as their online presence must generally be accessible to third parties. The following technical and organisational measures are intended to ensure that the information provided by the HFBK online can remain accessible to the public while also ensuring adequate levels of protection for the university's information technology infrastructure, especially in protecting the university against cyber-attacks.

The responsibilities of the university's Management Team and its data security officers are set out below. In addition, all members and affiliates of the university have a responsibility to ensure that they play their part in maintaining data security.

2
Task and role of the Senior Management Team in relation to data security

The university's senior management team (SMT) regularly evaluates the risk of cyber-attacks and is responsible for the overall defensive strategy employed by the university. The SMT initiates, steers and monitors the university's security procedures and is responsible for the provision of the resources needed for managing data security and assessing their value for money in accordance with its financial responsibilities. Overall responsibility for data security rests with the SMT. Operational tasks can be delegated by the SMT. In addition, the SMT must ensure that university staff are kept up to date on their own responsibilities in maintaining data security.

3
Responsibilities and tasks of the data security officer

The HFBK Hamburg has a data security officer. Their role includes, especially,

- Advising and supporting the SMT on questions of data security and submitting regular reports on the university's data security status;
- Leading and assisting in creating and updating security strategies and relevant associated strategies along with further guidelines and overseeing their implementation, and/or coordinating projects in relation to data security;
- Investigating possible security breaches, and initiating and coordinating campaigns and training to raise awareness of data security and best practice.

4
Recognising and preventing cyber-attacks

Attacks on university IT systems often take the form of “social engineering” and/or through an infiltration of the system with malware (malicious software). In these cases, attempts are made to obtain access to information on a fraudulent basis, e.g., through phishing emails or scam calls, or to infiltrate existing systems through installing software that then provides access to a protected IT system.

The following situations may indicate that someone is attempting to hack into the system:

- An email containing a link or an attachment from an unknown sender, and/or where the contents do not make sense or have no connection with the sender;
- A communication (email, text message or similar) asking for confidential information or log-in details.

If you think something is wrong:

- Never open the attachment or click on the link! Opening the attachment or clicking on a link could trigger the installation of malware capable of unlocking your local data and network drives.
- If you do not recognise the sender, delete the email.
- If you recognise the sender, but the email still seems suspicious, do not open any attachments. Ask the person named as the sender whether they recognise the email and, if they did not send it, inform the IT department.
- If you have the impression that the email has been sent in an attempt to gain access to protected information, you must inform the data security officer or data protection officer immediately.

5
How to recognise and respond to a cyber-attack

The following device behaviour may indicate that a device has been infected with malware:

- Programmes crash frequently, the system behaves unpredictably, or you receive multiple error messages (especially in relation to your operating system, MS Office applications, etc.).
- Icons or file contents change for no apparent reason.
- The amount of data storage on the device(s) keeps decreasing.
- The device sends emails on its own, without any human input.
- Files disappear or cannot be opened.
- You are unable to access drives or data storage devices.
- Problems starting up the IT system.
- Problems with amending or saving files.

If you think something is wrong:

- Disconnect your IT system from the network (unplug the network cable, shut down the Wi-Fi connection). Do not continue to work in the system.
- Use a different device to report the problem to the HFBK Hamburg's IT department via support@HFBK.net, and await further instructions.

The IT department is the first point of contact in any situation where IT devices are behaving differently to normal.

6
Software on work devices

To protect university-internal information and the university's IT infrastructure, software may only be installed on HFBK devices if it is needed for work-related activities.

You must contact the IT department before installing any software on university devices, especially if you wish to download software from the internet or activate software that you have received by email. This is to ensure that the software does not pose a risk to the HFBK IT system.

7
Use ArtCloud in preference to external cloud storage

Files that are saved as part of your work or studies at the HFBK should be saved to the HFBK's internal cloud storage, ArtCloud (https://artcloud.hfbk.net). ArtCloud meets all data security and IT security requirements and must be used in preference to other cloud storage options wherever possible.

The use of external cloud storage services (e.g., Microsoft Teams, Slack, Dropbox, Google-Drive etc.) risks breaches of data security such as the illegal processing of information by third parties and the infringement of data protection legislation.

8
Limited use of personal hardware and software

In future, users will be able to access HFBK Hamburg Wi-Fi on their own devices (e.g. laptops, smartphones) through the central service Eduroam. You can register for Eduroam using your HFBK log-in details. External guests can obtain a temporary visitor log-in from the IT department. Other services can be used if they are available as a browser app.

The HFBK cannot provide technical support for personal hardware and software. University licences must not be installed on personal devices.

9
Clean Desk and Clear Screen

Anyone who is intending to be away from their usual place of work for substantial periods of time (e.g., because of meetings or travel), or who is leaving the university premises for the day, must ensure that any sensitive, confidential information is kept secure and cannot be accessed by third parties. Please ensure that:

- Printed documents containing confidential information are not left on your desk or on printers/scanners;
- Mobile devices and storage devices (e.g., USB sticks, external hard drives) are put away;
- Your screen is locked, even if you are leaving your desk for just a few minutes;
- No passwords or other log-in information are left visible/accessible.

10
Data backups

Data backups take place regularly to ensure that data are not lost through human error, technical problems, etc. As a general principle, data must be stored on the university's central servers (network drives or ArtCloud). You should ensure that you are informed of the times and procedures in relation to centralised backups and when these are scheduled for your department.

You are responsible for ensuring that your data are stored securely if they cannot be stored on central servers.

11
Information transfer (especially for work-related purposes)

To ensure that all HFBK-related content remains confidential when it is sent internally or externally, the following guidelines are to be followed:

- Before sending confidential information (for example to external suppliers), you must check whether a confidentiality and/or non-disclosure agreement is required.
- Emails will not be automatically forwarded to external email addresses.
- Confidential discussions must not be held in public spaces or via unsecured communication channels.
- All confidential information must be sent encrypted.
- External, public services such as file-sharing (e.g., Dropbox, OneDrive, GoogleDrive) must not be used to share personal and/or confidential data. ArtCloud, the service provided by the HFBK Hamburg, is available for sharing files and other information.

12
Deleting confidential information/documents and re-using technological devices

Confidential information belonging to the HFBK Hamburg may be held on print-outs, computers and external storage devices. This information must be securely saved and then deleted from any device that is being transferred to another person, exchanged or repaired.

- Print-outs containing confidential information must be disposed of using the shredders that have been set up locally. If this cannot be done immediately, the print-outs must be kept in a secure facility (e.g., a data protection bin) until it is possible to destroy them.
- Defunct IT devices belonging to the HFBK Hamburg must be handed back to the IT department.
- IT devices may only be re-used or disposed of by the IT department, and only when all information stored on them has been deleted.

13
Avoiding risks when using mobile devices outside the HFBK Hamburg

The use of mobile devices outside university premises can lead to the following risks:

- Loss, theft or inappropriate use of the device;
- Illegal third-party access and/or the device being used by or disposed of by third parties.

To minimise these risks, please observe the following rules:

- HFBK devices may not be lent to third parties. Any use of laptops/computers by a third party may only take place under the supervision of the device owner.
- Each user is responsible for saving work-related information on their personal network drive and/or to ArtCloud. Shortcuts that are not needed (e.g. Bluetooth, Wi-Fi) must be deactivated.

The loss of a HFBK device must be reported to the IT department immediately.

14
Entry into force

The Information Security Policy of the HFBK Hamburg enters into force on 28 February 2024.

Executive Committee, HFBK Hamburg

Annex

Recommendations for creating/assigning passwords

To ensure that passwords are as strong as possible, the following rules apply:

- Passwords must never be shared with or accessible to third parties.
- Passwords must be created by the user of the relevant device/programme.
- Do not use the same password for multiple authentication processes (e.g. HFBK log-in/Apple ID/Google ID/Microsoft Office etc.)
- The initial or re-set password assigned by the IT department must be changed as soon as possible.
- Multiple passwords must be saved in a "password safe", not on internet browsers, unsecured files or in hard copy (unless they are stored in a sealed envelope in a safe).
- If there is any possibility that the password has been accessed by a third party, it must be changed immediately and the IT department must be informed.

The strength of a password is dependent above all on its complexity and length. A password must meet the following criteria:

- It must contain at least 16 characters.
- It must not be easy to guess, and should not contain any of the following:
    - Your name or username
    - Your birthday, date of birth or car registration.
    - Sequences of numbers or characters that appear consecutively on the keyboard (e.g., QWERTZ, 23456)
    - Years (e.g. 2024)
    - Whole words that are used frequently
    - Phrases or words connected to the HFBK or HFBK projects
    - Words that appear in the dictionary.