Informationssicherheitsrichtlinie der HFBK Hamburg

Das Präsidium der Hochschule für bildende Künste erlässt die nachstehende Richtlinie:

§ 1
Hintergrund, Zweck und Anwendungsbereich

Hochschulen mit ihrer für Dritte offenen Struktur stellen im Hinblick auf die Informationssicherheit eine große Herausforderung dar. Die nachfolgenden technischen und organisatorischen Maßnahmen sollen helfen, die technische Offenheit der HFBK Hamburg zu bewahren und trotzdem ein ausreichendes Sicherheitsniveau der Hochschul-IT insbesondere gegenüber Cyberangriffen gewährleisten zu können.

Die im folgenden genannte Verantwortung der Hochschulleitung und der für die IT-Sicherheit Beauftragten entbindet die Mitglieder und Angehörigen der Hochschule nicht von einem eigenen verantwortungsvollen Verhalten.

§ 2
Aufgabe und Rolle der Hochschulleitung in Bezug auf IT-Sicherheit

Die Hochschulleitung bewertet regelmäßig das potentielle Risiko durch Cyberangriffe und gibt den Rahmen zur Gefahrenabwehr vor. Sie initiiert, steuert und kontrolliert den Sicherheitsprozess an der Hochschule und stellt die erforderlichen Ressourcen für das Sicherheitsmanagement, in Abwägung von Aufwand und Ertrag, bereit. Die Gesamtverantwortung zur IT-Sicherheit liegt bei der Hochschulleitung. Operative Aufgaben können durch die Hochschulleitung delegiert werden, zudem sollen die Mitarbeiter*innen zu sicherheitsbewusstem Verhalten regelmäßig informiert werden.

§ 3
Zuständigkeiten und Aufgaben des/der Informationssicherheitsbeauftragten

Die HFBK Hamburg verfügt über eine/n Informationssicherheitsbeauftragte/n, die/der insbesondere

- die Hochschulleitung in IT-Sicherheitsfragen berät und unterstützt sowie regelmäßig über den Status der Informationssicherheit berichtet,
- bei der Erstellung und Aktualisierung von Sicherheitskonzepten und zugehöriger Teilkonzepte sowie weiterer Richtlinien – ggf. auch federführend – mitwirkt und die Implementierung begleitet bzw. sicherheitsrelevante Projekte koordiniert,
- sicherheitsrelevante Vorfälle untersucht sowie Sensibilisierungen und Schulungen zur Informationssicherheit initiiert und koordiniert.

§ 4
Versuche von Angriffen auf die IT erkennen und verhindern

Angriffe auf eine Hochschul-IT werden häufig in Form des sogenannten „Social Engineering" bzw. durch Einschleusen einer Schadsoftware durchgeführt. Dabei wird versucht, durch Täuschung, z. B. in Form einer falschen Nachricht oder eines Anrufs, von Personen Zugangsinformationen zu erhalten oder Software einzuspielen und dadurch Zugang zu dem geschützten IT-System zu erhalten.

Folgende Situationen können auf den Versuch eines Angriffs hindeuten:

- E-Mail mit Link oder Anhang, deren Absender unbekannt oder deren Inhalt nicht plausibel ist oder in keinem Zusammenhang zum Absender steht.
- Nachricht (E-Mail, SMS o.ä.), in der nach vertraulichen Informationen oder Zugangsdaten gefragt wird.

Verhalten im Verdachtsfall:

- In keinem Fall den Anhang oder Link einer E-Mail öffnen! Hierdurch könnte eine Schadsoftware ausgeführt werden, die z. B. zur Entschlüsselung ihrer Daten lokal und auf Netzwerklaufwerken führen kann.
- Sofern die Absenderadresse unbekannt ist, ist diese E-Mail zu löschen.
- Falls die Absenderadresse bekannt ist, die E-Mail aber verdächtig erscheint, sollten keine Anhänge geöffnet werden, sondern bei der absendenden Person nachgefragt und ggf. die IT-Abteilung informiert werden.
- Wenn der Eindruck entsteht, dass auf geschützte Informationen unberechtigter Zugriff erhalten werden soll, sollten Nutzer*innen sich sofort an die/den Datenschutzbeauftragte*n oder die für Informationssicherheit Beauftragten wenden.

§ 5
Erkennen und Handeln im Fall eines Cyberangriffs

Folgende Situationen können auf eine erfolgte Infektion mit Schadsoftware hindeuten:

- häufige Programmabstürze, unerklärliches Systemverhalten oder Fehlermeldungen (insb. Betriebssystem, Office-Anwendungen, etc.),
- unerklärliche Veränderungen von Icons oder Dateiinhalten,
- ständige Verringerung des freien Speicherplatzes,
- Versand von E-Mails ohne Aktion durch die Anwender*innen,
- nicht auffindbare oder verschlüsselte Dateien,
- kein Zugriff auf Laufwerke oder Datenträger,
- Probleme beim Starten des IT-Systems,
- Probleme beim Verändern oder Abspeichern von Dateien.

Verhalten im Verdachtsfall:

- IT-System vom Netz trennen (Netzwerkkabel ziehen oder WLAN-Verbindung trennen) und nicht mehr am System weiterarbeiten.
- Meldung an die IT-Abteilung der HFBK Hamburg über support@HFBK.net (nicht vom betroffenen Gerät) und auf weitere Anweisungen warten.

Die IT-Abteilung ist als erste Anlaufstelle über jegliche Art von ungewöhnlichem Verhalten von IT- Geräten zu informieren.

§ 6
Software auf dienstlichen Geräten

Auf allen HFBK-eigenen IT-Geräten darf zum Schutz der hochschuleigenen Informationen und der IT-Infrastruktur nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist.

Vor dem Einspielen, insbesondere auch vor dem Herunterladen von Software aus dem Internet oder dem Starten von per E-Mail erhaltener Software auf Rechnern der Hochschule ist Rücksprache mit der IT-Abteilung zu halten um sicherzustellen, dass von dieser Software keine Gefährdung für das IT-System ausgeht.

§ 7
Vorrang der Nutzung der Art-Cloud

Zur gemeinsamen Dokumenten-Ablage im HFBK-Kontext steht die HFBK-interne ArtCloud (https://artcloud.hfbk.net) zur Verfügung. Die ArtCloud erfüllt alle datenschutzrelevanten und IT-Sicherheitsanforderungen und soll möglichst ausschließlich genutzt werden.

Bei der Nutzung von externen Cloud-Diensten (z. B. Microsoft Teams, Slack, Dropbox, Google Drive etc.) besteht bei der Verarbeitung von Informationen durch unberechtigten Zugriff Dritter und die Verletzung datenschutzrechtlicher Vorgaben ein erhöhtes Sicherheitsrisiko.

§ 8
Einschränkungen bei der Nutzung von privater Hard- und Software

Mit privaten Endgeräten (Laptops, Smartphones) kann das WLAN der HFBK Hamburg in Zukunft über den zentralen Dienst Eduraom, genutzt werden. Die Anmeldung erfolgt mit der HFBK Nutzerkennung. Externe Gäste können bei der IT-Abteilung temporäre Zugänge erhalten. Weitere Dienste sind immer dann nutzbar, wenn sie als Browser-Anwendung zur Verfügung stehen.

Für private Hard- oder software kann kein Support zur Verfügung gestellt werden. Hochschullizenzen werden nicht auf private Endgeräte aufgespielt.

§9
Vorgaben zum Clean Desk und Clear Screen

Bei längerer Abwesenheit (z. B. Meetings, Termine außer Haus) oder bei Arbeitsende sind beim Verlassen des Arbeitsplatzes in der HFBK Hamburg alle sensiblen und vertraulichen Informationen vor dem unberechtigten Einblick oder Zugriff Dritter zu schützen:

- ausgedruckte Dokumente mit vertraulichen Informationen dürfen nicht auf dem Schreibtisch oder in der Ablage von Multifunktionsgeräten verbleiben,
- mobile IT-Geräte oder Speichermedien (z.B. USB-Sticks oder mobile Festplatten) sind wegzuräumen,
- der Sperrbildschirm ist bei jedem, auch kurzfristigen, Verlassen des Arbeitsplatzes zu aktivieren,
- am Arbeitsplatz dürfen keine Passwörter oder andere Zugangsinformationen hinterlegt werden.

§ 10
Datensicherung

Regelmäßig durchgeführte Datensicherungen schützen vor Verlust durch Fehlbedienung, technische Störungen etc. Grundsätzlich sind Daten auf zentralen Servern (Netzlaufwerk oder Art Cloud) der Hochschule zu speichern. Bei zentraler Datensicherung sollten sie sich über die in den jeweiligen Bereichen geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung informieren.

Ist die Speicherung auf zentralen Servern nicht möglich, sind die Nutzer*innen für die Sicherung ihrer Daten selbst verantwortlich.

§ 11
Informationsübertragung, insbesondere bei dienstlichen Angelegenheiten

Zur Aufrechterhaltung der Vertraulichkeit bei der internen und externen Kommunikation HFBK-bezogener Inhalte gelten folgende Vorgaben:

- vor dem Versand von vertraulichen Informationen (z. B. an externe Dienstleister*innen) wird geprüft, ob eine Vertraulichkeits- oder Geheimhaltungsvereinbarung abzuschließen ist,
- E-Mails werden nicht automatisch an externe E-Mail-Adressen weitergeleitet,
- vertrauliche Gespräche werden nicht in der Öffentlichkeit oder über unsichere Kommunikationskanäle geführt,
- vertrauliche Informationen sollen ausschließlich verschlüsselt versendet werden,
- externe öffentliche Dienste wie Filesharing (z. B. Dropbox, OneDrive und Google Drive etc.) werden nicht für personenbezogene oder vertrauliche Daten genutzt, dafür steht die ArtCloud der HFBK Hamburg zur Verfügung.

§ 12
Entsorgung von vertraulichen Informationen/Dokumenten und Weiterverwendung technischer Geräte

Vertrauliche Informationen der HFBK Hamburg werden auf Ausdrucken, Rechnern und Datenträgern gespeichert. Diese Informationen sind vor Weitergabe eines Geräts, Austausch oder Reparaturen zu sichern und zu löschen:

- Ausdrucke mit vertraulichen Inhalten sind über aufgestellte Aktenvernichter zu entsorgen oder bis zur Vernichtung in verschlossenen Einrichtungen (z. B. Datenschutztonne) zu sichern,
- funktionsunfähige IT-Geräte der HFBK Hamburg müssen der IT-Abteilung übergeben werden,
- Weitergabe oder Entsorgung von IT-Geräten darf nur durch die IT-Abteilung und erst nach Löschung der darauf gespeicherten Informationen erfolgen.

§ 13
Vermeidung von Risiken bei der Nutzung mobiler IT-Geräte außerhalb der HFBK Hamburg

Beim Einsatz mobiler Geräte außerhalb der HFBK Hamburg entstehen Risiken durch:

- Verlust, Diebstahl oder unsachgemäßen Gebrauch des Geräts,
- unberechtigten Zugriff auf des bzw. Weitergabe oder Entsorgung des Geräts.

Die Einhaltung nachfolgender Regeln soll die oben genannten Risiken minimieren:

- HFBK-eigene Geräte dürfen nicht an Dritte verliehen werden, die Nutzung von Laptops/Rechnern durch Dritte erfolgt ausschließlich unter Aufsicht der besitzhabenden Person.
- Es liegt in der Verantwortung der anwendenden Person, dienstliche Daten immer auf dem persönlichen Netzlaufwerk bzw. in der ArtCloud zu sichern und nicht benutzte Schnittstellen (Bluetooth, WLAN) sind zu deaktivieren.

Der Verlust eines HFBK-eigenen Geräts muss umgehend der IT-Abteilung gemeldet werden.

§14
Inkrafttreten

Die Informationssicherheitsrichtlinie der HFBK Hamburg tritt am 28.02.2024 in Kraft.

Das Präsidium der HFBK Hamburg

Anhang

Empfehlungen zur Passwort-Vergabe:

Um sicherzustellen, dass Passwörter möglichst sicher gewählt werden, sind folgende Regeln im Umgang mit und bei der Vergabe von Passwörtern zu beachten:

- Passwörter dürfen für Dritte nicht einsehbar sein oder mit Dritten geteilt werden,
- Passwörter müssen selbst gewählt werden,
- es dürfen keine identischen Passwörter für unterschiedliche Authentifizierungsstellen (z. B. HFBK- Login, Apple-ID, Google-ID, Office365, …) verwendet werden,
- Initialpasswörter und von der IT-Abzteilung zurückgesetzte Passwörter sind schnellstmöglich zu ändern,
- Passwörter dürfen nur in einem „Passwortsafe“ gespeichert werden, nicht in Internetbrowsern, unverschlüsselten Dateien oder in Papierform (ausgenommen davon ist die Ablage in einem verschlossenen Umschlag mit Lagerung in einem Safe),
- bei Verdacht auf Missbrauch muss das Passwort unverzüglich geändert und die IT-Abteilung informiert werden.

Die Sicherheit eines Passwortes ist sehr stark abhängig von dessen Komplexität und Länge. Bei der Wahl des Passwortes sind folgende Regeln zu beachten:

- Das Passwort muss mindestens aus 16 Zeichen bestehen,
- Das Passwort darf nicht leicht zu erraten sein, d. h. es sollte möglichst nicht enthalten:
- Name oder Kontoname der/des Mitarbeitenden,
- Geburtstag oder Kfz-Kennzeichen,
- Aufeinanderfolgende Zeichen- oder Zahlenfolgen auf der Tastatur (z. B. QWERTZ, 23456),
- Jahreszahlen,
- Ganze, gebräuchliche Wörter,
- Begrifflichkeiten, die mit der Hochschule und deren Projekten in Verbindung stehen,
- im Wörterbuch enthaltene Wörter.