Informatik-Richtlinie

Beispiel Label Cyber-Safe

Hinweis: Dieses Dokument wird im Rahmen der Cyber-Safe-Labellisierung zur Verfügung gestellt und muss an Ihre Situation angepasst werden. Seine Verwendung garantiert nicht, dass die Anforderungen des Labels erfüllt werden.

1 Ziel

Dieses Dokument legt die Regeln für den Zugriff auf und die Nutzung von IT-Ressourcen fest.

ausschliesslich zu beruflichen Zwecken, sofern in dieser Richtlinie keine Ausnahme vorgesehen ist. Zur Transparenz gegenüber den Benutzenden und zur Förderung einer fairen, verantwortungsvollen und sicheren Nutzung der Systeme definiert diese Richtlinie die Nutzungsregeln sowie die Kontroll- und Überwachungsmöglichkeiten, nicht nur im Rahmen der Arbeitsvertragserfüllung, sondern auch im Hinblick auf die zivil- und strafrechtliche Verantwortung des Arbeitgebers. Sie ersetzt nicht die geltenden gesetzlichen Bestimmungen.

2 Anwendungsbereich

Die IT-Richtlinie gilt für alle Mitarbeitenden, Praktikanten usw. (im Folgenden Benutzende genannt), die zur Nutzung der IT-Ausstattung des Labels Cyber-Safe berechtigt sind.

Jeder Benutzende verpflichtet sich ausdrücklich, die Bestimmungen dieses Dokuments einzuhalten.

3 Pflichten des Arbeitgebers

Der Arbeitgeber verpflichtet sich, im Rahmen der Massnahmen zum Schutz seiner Interessen und bestimmter IT-Geräte die Persönlichkeit der Benutzenden zu respektieren und zu schützen. Private Daten der Benutzenden werden nicht eingesehen, soweit sie als solche erkennbar sind (z. B. Betreffzeile, Ordner- oder Dateiname).

In der Cybersicherheit ist die Wachsamkeit der Mitarbeitenden eine der besten Barrieren gegen Eindringlinge. Benutzende müssen daher verdächtige Vorfälle oder Anzeichen einer Daten- oder Gerätekompromittierung sofort dem IT-Support oder der Leitung melden: verdächtige E-Mails, ungewöhnliche Nachrichten, nicht zugängliche Ressourcen, Dateien mit merkwürdigem Inhalt, Fenster, die eine unautorisierte Remote-Verbindung anzeigen, Antivirus-Meldungen usw. Der Arbeitgeber behandelt diese Informationen vertraulich.

4 Pflichten der Benutzenden

4.1 Sicherheitsregeln: Zugriffsrechte

Der Zugriff auf IT-Ressourcen erfolgt über ein **persönliches, nicht übertragbares** Benutzerkonto. Dieses muss durch ein sicheres Passwort geschützt sein (mindestens 12 Zeichen, Klein- und Grossbuchstaben, Zahlen, Sonderzeichen, mindestens ein Zeichen jeder Kategorie) und darf keine leicht ableitbaren Informationen über den Benutzenden enthalten (Name, Vorname, private Passwörter) und darf zudem **keine Passwörter enthalten, die (ganz oder teilweise) privat verwendet werden**.

Zwei-Faktor-Authentifizierung ist verpflichtend. Authentifizierungsmittel sind strikt persönlich (Telefon, private E-Mail, …) und passwortgeschützt. Passwörter dürfen nicht weitergegeben werden. Benutzende dürfen nur autorisierte Konten verwenden.

Benutzende verbinden sich nicht mit öffentlichem WLAN ohne VPN; alternativ wird die mobile Verbindung geteilt.

4.2 Vertraulichkeitspflicht

Der Zugang der Benutzenden zu Informationen und Dokumenten, die auf den IT-Systemen und Netzwerken gespeichert sind (einschliesslich Internet), ist auf die eigenen, öffentlichen oder geteilten Informationen beschränkt. Es ist insbesondere verboten, absichtlich Kenntnis von Informationen zu nehmen, die über Netzwerke übertragen werden oder von anderen Benutzenden gehalten werden, selbst wenn diese sie nicht geschützt haben.

4.3 Software: Installation und Kopien

Software darf nur mit Zustimmung des Webmasters installiert werden.

Private Cloud-Speicher (z. B. Dropbox, Google Drive) sind verboten.

Private Kopien oder Installationen lizenzierter Software des Labels Cyber-Safe sind nicht erlaubt.

4.4 Arbeitsplätze und zugehörige Geräte

Änderungen am Netzwerk und an den Verbindungsleitungen: Änderungen werden nur vom Webmaster oder von einer von ihm/ihr autorisierten Person vorgenommen.

Änderungen an den Konfigurationen: Änderungen werden nur vom Webmaster oder von einer von ihm/ihr autorisierten Person vorgenommen.

4.5 Private Geräte

Benutzende verwenden ausschliesslich der beruflichen Ausstattung, die für die Ausübung der beruflichen Tätigkeit zur Verfügung gestellt wird.

Es ist untersagt, private elektronische Geräte, wie insbesondere Smartphones, USB-Sticks, externe Systeme oder Tablets, an den Arbeitsplatz oder an irgendeinen Computer im Netzwerk anzuschliessen.

Benutzende, die ausnahmsweise ein privates Gerät (Laptop etc.) an das IT-Netzwerk anschliessen möchten, müssen die Genehmigung mit Begründung bei der Geschäftsleitung oder beim Webmaster einholen.

Die Office-Suite darf nicht über das berufliche Konto auf einem privaten Gerät installiert werden, und die Dateien des Labels Cyber-Safe dürfen dort nicht synchronisiert werden. Die Konfiguration der E-Mail auf eigenen Geräten ist jedoch erlaubt.

Falls zwingend auf einem nicht beruflichen Gerät gearbeitet werden muss, darf ausschliesslich Office Online (im Browser) verwendet werden.

4.6 Meldung von Vorfällen

Um einen optimalen Betrieb der Infrastrukturen und gute Arbeitsbedingungen für alle zu gewährleisten, sind die Mitarbeitenden angehalten, sofort jede technische Störung, Ausfall oder Beschädigung zu melden (z. B. Verlust der Netzwerkverbindung, defektes oder beschädigtes Gerät, Geräusche, Rauch oder andere verdächtige Elemente an einem PC oder Zubehör). Dies ermöglicht dem IT-Support oder der verantwortlichen

Person, schnell zu reagieren und gegebenenfalls den Techniker zu kontaktieren oder Ersatzteile zu bestellen.

Der Verlust, das Vergessen oder der Diebstahl, insbesondere eines Laptops, Tablets, Smartphones oder eines Speichermediums (Festplatte, USB-Stick, Speicherkarte…), an einem bekannten oder unbekannten Ort, muss unverzüglich dem IT-Support gemeldet werden.

In der Cybersicherheit ist die Wachsamkeit der Mitarbeitenden eine der besten Barrieren gegen Eindringlinge! Es ist daher unerlässlich, dass Benutzende aufmerksam bleiben und sofort dem IT-Support oder der Geschäftsleitung jedes verdächtige Element oder jeden Verdacht auf Daten- oder Geräte Kompromittierung melden: verdächtige E-Mails, ungewöhnliche Nachrichten, nicht zugängliche Ressourcen, Dateien mit merkwürdigem Inhalt, Fenster, die eine unautorisierte Remote-Verbindung anzeigen, Antivirus-Meldungen usw.

Wenn jemand glaubt, auf einen falschen Link oder eine verdächtige Stelle in einer E-Mail geklickt zu haben, ist es entscheidend, nicht in Panik zu geraten und das Problem nicht zu verharmlosen oder zu verschweigen, sondern die Information sofort weiterzuleiten, damit Kontrollen durchgeführt und gegebenenfalls die „Türen“ rechtzeitig geschlossen werden können.

5 Internet

5.1 Grundprinzipien

Das Internet darf von Benutzenden ausschliesslich zu beruflichen Zwecken und im Rahmen der ihnen zugewiesenen Aufgaben genutzt werden.

Die Nutzung des Internets zu privaten Zwecken ist erlaubt, sofern der Ressourcenverbrauch gering ist und weder die Arbeitszeit noch die Netzwerkkapazität beeinträchtigt werden. Private Nutzung muss per Definition gelegentlich und nebensächlich bleiben.

Die Verbreitung persönlicher oder werblicher Informationen, die nicht mit der beruflichen Tätigkeit in Zusammenhang stehen, ist strikt verboten.

Benutzende dürfen keine kostenpflichtigen Informationsdienste abonnieren, es sei denn, es liegt eine vorherige Genehmigung vor.

5.2 Missbräuchliche Nutzung

Alle Benutzenden müssen sicherstellen, dass sie das Internet nutzen, ohne dem Label Cyber-Safe rechtliche, regulatorische oder operationelle Risiken zuzufügen und ohne den Ruf der Organisation zu gefährden. Jede missbräuchliche oder illegale Nutzung ist strikt verboten. Der Zugriff, das Hoch- oder Herunterladen sowie die Übertragung von Daten, deren Inhalt gesetzeswidrig, unethisch, unmoralisch oder beleidigend, demütigend oder abwertend ist, sind ausdrücklich untersagt.

Der Arbeitgeber behält sich das Recht vor, ohne Vorankündigung den Zugang zu bestimmten Kategorien von Webseiten zu blockieren, insbesondere:

- Nicht-berufliche E-Mail-Dienste, einschliesslich Instant-Messaging-Dienste („Chat“);
- Finanztransaktionsseiten (einschliesslich Börsenseiten) oder kostenpflichtige Seiten;
- Spiel- und Wettseiten;
- Seiten mit erotischem, gewalttätigem, rassistischem oder in sonstiger Weise sittenwidrigem Inhalt;
- Seiten, die die Informationssysteme übermässig beanspruchen (z. B. Verbindung zu Radiosender-Webseiten).

5.3 Herunterladen von Informationen

Software, Daten und Dateien (einschliesslich Dateien mit Audio- oder Videoinhalten oder beidem) dürfen nur dann aus dem Internet auf die Netzwerke heruntergeladen werden, wenn sie in Zusammenhang mit der beruflichen Tätigkeit stehen. Diese Vorgänge sind erlaubt, wobei Benutzende sicherstellen müssen, dass die Rechte Dritter respektiert werden und keine Viren ins Netzwerk eingeschleust werden.

Benutzende verpflichten sich, keine Software oder Dateien, die durch Copyright geschützt sind (Musik, Filme etc.), illegal zu kopieren, keine Informationen Dritter ohne deren Genehmigung zu verbreiten und bei Nutzung von Informationen die Quellen anzugeben.

5.4 Elektronische Kommunikation

Benutzende verwenden ihre im E-Mail-System des Labels Cyber-Safe registrierte Adresse für alle beruflichen Kommunikationszwecke. Sie achten darauf, ihre Nachrichten korrekt zu formulieren, da der Name des Labels Cyber-Safe in der Adresse erscheint.

Massensendungen (Kettenmails) oder die Weiterleitung von Adressverzeichnissen (Spam) sind verboten.

Die Übermittlung vertraulicher Inhalte (im Nachrichtentext oder als Anhang) muss verschlüsselt erfolgen.

Benutzende verpflichten sich, ihr berufliches E-Mail-Konto möglichst nicht für private Zwecke zu nutzen. Falls doch, müssen E-Mails mit dem Präfix „privat“ versehen oder in einen Ordner mit der Bezeichnung „privat“ verschoben werden. Andernfalls gelten diese E-Mails als beruflich.

5.5 Zugriffsrechte / Passwort

Der Zugriff auf IT-Ressourcen und Dateien wird über ein **persönliches, nicht übertragbares** Konto gewährt.

Bereitstellung von Bitwarden:

Um die Sicherheit unserer Informationen zu erhöhen, stellt das Label Cyber-Safe allen Mitarbeitenden das Passwort-Management-Tool Bitwarden zur Verfügung.

- Alle Passwörter, die im Rahmen der beruflichen Tätigkeit verwendet werden, müssen unbedingt in Bitwarden gespeichert werden.

- Beim Erstellen eines neuen Passworts ist die in Bitwarden integrierte Passwortvorschlagsfunktion zu nutzen, um ein optimales Sicherheitsniveau zu gewährleisten.

- Passwörter dürfen nicht im Webbrowser (Chrome, Edge, Safari, …) gespeichert werden.

Bei Fragen oder Unsicherheiten zur Nutzung von Bitwarden ist der IT-Support zu kontaktieren.

Alle Zugänge, insbesondere das Bitwarden-Passwort, müssen durch ein sicheres Passwort geschützt werden, das mindestens 12 Zeichen umfasst, Klein- und Grossbuchstaben, Zahlen sowie Sonderzeichen enthält, mindestens je ein Zeichen jeder Kategorie. Ausserdem darf es weder Name, Vorname noch andere leicht ableitbare Informationen über die Benutzenden enthalten und darf zudem **keine Passwörter enthalten, die (ganz oder teilweise) privat verwendet werden.**

Vorschlag für die Erstellung eines starken Passworts:

- Die ersten Buchstaben eines einfachen Satzes nehmen

- Ohne Bezug zu persönlichem Leben/Familie

- Mit einem Zeichen zur Markierung der Leerstellen

- Einige Buchstaben durch ähnlich aussehende Zahlen ersetzen

- Die Länge sollte 12 bis 16 Zeichen betragen

Beispiel: „Europa Park! Ich Liebe“ wird zum starken Passwort: **3u.Pa! Ic.Li.**

Passwörter dürfen nicht weitergegeben werden. Benutzende nutzen nur die Konten, für die sie autorisiert wurden. Konten, ob intern oder Kundenkonten, dürfen keinesfalls übertragen werden.

Die gleichen Regeln gelten für Passwörter von Internetseiten, die beruflich genutzt werden. Zwei-Faktor-Authentifizierung ist zu bevorzugen. **Das Passwort der Benutzer-Session darf keinesfalls wiederverwendet werden.**

5.6 Software mit Künstlicher Intelligenz (KI)

Generative KI, wie ChatGPT oder Bard, kann ein leistungsfähiges Werkzeug für berufliche Tätigkeiten sein. Ihre Nutzung muss jedoch kontrolliert erfolgen, um unbeabsichtigte Folgen wie die ungewollte Weitergabe personenbezogener, sensibler oder vertraulicher Daten zu vermeiden. Dieses Dokument liefert Richtlinien für eine verantwortungsvolle und ethische Nutzung dieser Technologie.

Risiken und zulässige Nutzung:

- **Lizenzen**: Das Label Cyber-Safe verfügt über Lizenzen für die Nutzung von ChatGPT; die Nutzung ist nur über diese Label-Konten erlaubt.
- **Generierter Inhalt:** Generative KI kann menschenähnliche Texte erzeugen. Es ist jedoch wichtig zu beachten, dass solche Systeme voreingenommene oder unangemessene Inhalte erzeugen können. Mitarbeitende des Labels Cyber-Safe müssen diese Technologien daher mit Vorsicht und Diskretion nutzen und den Inhalt beherrschen.
- **Sensiblen Daten:** Es ist davon auszugehen, dass ALLE Informationen, die in generative KI-Systeme eingegeben werden, Teil ihres Trainingsdatensatzes werden und auf Anfragen anderer Personen ausgegeben werden können. Daher dürfen personenbezogene, sensible, vertrauliche oder durch Datenschutzgesetze geschützte Informationen in keinem generativen KI-System eingegeben werden, unabhängig von den aktivierten Datenschutzkontrollen.
- **Unangemessene Inhalte:** Generative KI darf nicht zur Erstellung diffamierender, diskriminierender oder illegaler Inhalte verwendet werden.
- **Identitätsmissbrauch:** Generative KI darf nicht zur Nachahmung der Identität von Personen oder Organisationen verwendet werden.
- **Gesetzeskonformität:** Generative KI darf nicht zur Erstellung von Inhalten verwendet werden, die gegen Gesetze oder Vorschriften zum Datenschutz verstossen.
- **Ruf des Labels Cyber-Safe:** Generative KI darf nicht für Aktivitäten genutzt werden, die den Ruf des Labels Cyber-Safe gefährden.

Bei Fragen oder Bedenken ist der IT-Support zu kontaktieren.

5.7 Nutzung von Instant-Messaging-Diensten

Die Nutzung von Instant-Messaging-Diensten (WhatsApp, Slack, …) beim Label Cyber-Safe ist im Rahmen von Veranstaltungen oder Projekten toleriert, unter Einhaltung der folgenden Richtlinien:

- **Ausschliessliche Nutzung für operative Organisation:** WhatsApp-Gruppen dürfen nur zur Koordination und operativen Organisation von Veranstaltungen im Zusammenhang mit dem Label Cyber-Safe verwendet werden. Jede andere Nutzung ist streng verboten.

- **Keine kundenspezifischen Informationen:** Es ist verboten, berufliche Informationen in Instant-Messaging-Systemen (WhatsApp-Gruppen, Apple Messenger, Slack, …) zu teilen. Dies umfasst, ist aber nicht beschränkt auf, vertrauliche Informationen, sensible Daten, Projektdiskussionen oder sonstige Informationen zu den beruflichen Tätigkeiten des Labels Cyber-Safe.

- **Respekt der Privatsphäre:** Mitglieder der Gruppen müssen die Privatsphäre der anderen Teilnehmer respektieren. Persönliche Informationen dürfen nur mit ausdrücklicher Zustimmung der betreffenden Person geteilt werden.

- **Angemessenes Verhalten:** Alle Gruppenmitglieder müssen ein respektvolles und angemessenes Verhalten zeigen. Jegliche Form von Belästigung, Diskriminierung oder unangemessener Sprache ist strikt verboten.

- **Moderation und Überwachung:** Die Administratoren der Gruppen sind für die Moderation des Inhalts verantwortlich und müssen sicherstellen, dass die Nutzungsregeln eingehalten werden. Bei Regelverstössen müssen sofortige Massnahmen ergriffen werden.

- **Löschung der Gruppen:** Nach Abschluss der Veranstaltung müssen die Administratoren die Gruppen löschen, um die Gespräche zu entfernen und sicherzustellen, dass keine weiteren Diskussionen stattfinden.

Bei Fragen oder Problemen ist der IT-Support zu kontaktieren.

6 Kontrolle

Es ist von entscheidender Bedeutung für den Ruf des Labels Cyber-Safe und das reibungslose Funktionieren des Sekretariats, dass Benutzende die in dieser Richtlinie festgelegten Anweisungen einhalten.

Um die Einhaltung der Regeln zur Gewährleistung der Sicherheit und des Rufs des Labels Cyber-Safe zu überprüfen und das Label nicht rechtlichen, regulatorischen oder operationellen Risiken auszusetzen, werden stichprobenartige und anonyme Kontrollen durchgeführt.

Für diese Kontrollen beachtet die Geschäftsleitung, unterstützt durch den Webmaster, die Grundsätze des Datenschutzes und der Privatsphäre, wie sie in den geltenden gesetzlichen Bestimmungen vorgeschrieben sind. Das Verhalten einzelner Benutzender wird nur analysiert, wenn eine Unregelmässigkeit festgestellt wurde.

Wenn die Analyse der Protokolle eine missbräuchliche oder sogar rechtswidrige Nutzung der Systeme und Netzwerke zeigt, informiert die Geschäftsleitung alle Benutzenden über:

- Vermutungen über rechtswidrige Handlungen
- Getroffene Massnahmen, insbesondere die Erhebung von Informationen über einen bestimmten Zeitraum.

Wenn die Missbräuche anhalten, werden die gesammelten Daten namentlich ausgewertet.

7 Sanktionen

Jede missbräuchliche Nutzung des Internets und jedes Verhalten, das gegen die Bestimmungen dieser Richtlinie verstösst, ist ausdrücklich verboten. Verstossende Personen können Disziplinarmassnahmen bis hin zur Entlassung oder sogar zu rechtlichen Schritten erwarten.

Name und Vorname:

Ort und Datum:

Unterschrift:

Als Ergänzung zu Punkt 4.5 der obigen Richtlinie, nach Relevanz zu berücksichtigen:

Verwaltung privater Geräte:

Benutzende, die sich mit privaten Geräten mit den IT-Ressourcen der Organisation verbinden, garantieren:

- Ihre Unbedenklichkeit, d.h.:
    - Installation der Sicherheitsupdates des Softwareanbieters des Basissystems (OS)
    - Aktualisierung installierter Software-Suiten
    - Aktualisierung der Antivirenprogramme
    - Beachtung von Warnmeldungen
- Einhaltung aller geistigen Eigentumsrechte durch ihre Software und Dateien.
- Zugriff auf das Gerät muss durch einen Authentifizierungsmechanismus, wie ein Passwort oder einen Sperrcode, geschützt sein.

Benutzende, die Daten oder Zugriffe auf sensible Daten der Organisation auf privaten Geräten speichern, garantieren die Verschlüsselung ihrer Festplatte.

