Informationssicherheitskonzept Europa-Universität Viadrina	EUROPA-UNIVERSITÄT VIADRINA FRANKFURT (ODER)
Maßnahmenbezeichnung	Informationssicherheitskonzept
Dokumentenname	Kennwortrichtlinie
Verantwortlich	komm. Direktorin IKMZ
Wiedervorlage	Gemäß Dokumentenlenkung / Bei Bedarf
Erstellungs-/Änderungs-Datum	22.03.2022
Klassifizierung	Viadrina-intern

Inhalt

Zielsetzung

Um die Sicherheit der IT-Infrastrukturen sowie der IT-gestützten Hochschulprozesse optimal zu gewährleisten und somit Schaden von der Hochschule möglichst abzuwenden, ist ein sicheres Kennwort-Management sowie der sichere Gebrauch von Kennwörtern notwendig.

Dieses Dokument beschreibt die Kennwort-Regeln für alle IT-Systeme und Nutzer:innen innerhalb der Europa-Universität Viadrina.

Zielgruppe

Anwender dieses Dokuments sind alle für die Kennwortvergabe und -verwaltung zuständigen Beschäftigten, Nutzer:innen und Administrator:innen (zentraler und dezentraler Komponenten)

Definitionen & Abkürzungen

Definitionen

Kennwörter sind geheime Authentisierungsinformationen und dienen zur Verifizierung der Identität eines Benutzers.

Nutzer:innen sind alle Personen, die Zugangsdaten zu von der Viadrina angebotenen Diensten bekommen.

Abkürzungsverzeichnis/Glossar

ISB - Informationssicherheitsbeauftragter

BSI - Bundesamt für Sicherheit in der Informationstechnik

Verwaltung von Kennwörtern

Das IKMZ gewährleistet über die Verfahren zur Bereitstellung und Verwaltung von Nutzer:innen-Accounts und -Kennwörtern, dass zugewiesene Zugangsberechtigungen und -beschränkungen wirksam geschützt sind.

Ausnahmen von den hier definierten Grundsätzen bzw. Verfahren müssen schriftlich beantragt werden und bedürfen der Freigabe durch den ISB (z.B. Verwendung von Gruppenkonten).

Nachfolgende Grundsätze sind bei der Verwaltung von Kennwörtern anzuwenden:

- Es sind grundsätzlich personalisierte Accounts zu verwenden.
- Alle intern genutzten Kennwörter sind vollständig und ausschließlich in einem Passwort-Tresor, z. B. Bitwarden, KeyPass oder Firefox-Account zu hinterlegen. Bei den Passwort-Tresoren müssen Master-Passwörter aktiviert sein.
- Kennwörter sollen gut zu merken sein. Das BSI gibt Hilfestellungen bei der Auswahl sicherer und gut merkbarer Kennwörter.
- Kennwörter dürfen **nicht** enthalten: Namensbestandteile, Geburtsdaten, Namen von Haustieren oder Verwandten, nur einzelne Wörter (Apfel) oder Wortdoppelungen (ApfelApfel), Zahlenfolgen (12345) oder Buchstabenfolgen (qwertz), identische Buchstaben oder Zahlen (aaa / 111)
- Kennwörter müssen aus mindestens 12 Zeichen und 3 Zeichenarten bestehen.

- Für Kennwörter sind folgende Zeichen erlaubt
  - Kleinbuchstaben (a-z)
  - Großbuchstaben (A-Z)
  - Ziffern (0-9)
  - Nur folgende Sonderzeichen (- ! (# . $: % = ?) + *)
- Kennwörter haben grundsätzlich eine unbegrenzte Gültigkeitsdauer. Nur in begründeten Fällen (z. B. Verlust des Passwortes) wird ein Passwortwechsel durch das IKMZ erzwungen.
- Werksseitige Standard-Kennwörter (z. B. von Firewalls, Access Points, Managed Switches) von Software- oder Hardware-Herstellern müssen bei der erstmaligen Einrichtung geändert werden.

Anforderungen an die Kennwortverwaltung

- Erstmalig übergebene Kennwörter werden als einzigartige, temporäre Initial-Kennwörter erstellt und müssen bei der ersten Anmeldung vom Nutzer:innen geändert werden.
- Temporäre Kennwörter müssen den Nutzer:innen auf eine sichere Weise, d. h. über einen anderen Weg als die Mitteilung des Nutzername kommuniziert werden. Die Identität der Nutzer:innen muss überprüft werden, bevor die Übergabe von Anmeldedaten und Kennwörtern erfolgt; bei Studierenden erfolgt dies im Zuge des Immatrikulationsverfahrens, bei Mitarbeitenden beim Einstellungsvorgang.
- Kennwörter werden nie unverschlüsselt (im Klartext) gespeichert oder über das Netzwerk übertragen.
- Für Nutzer:innen-Accounts wird sichergestellt, dass nur Kennwörter verwendet werden können, die den in diesem Dokument genannten Qualitätsanforderungen entsprechen.
- Eine erneute Verwendung der 6 zuletzt verwendeten Kennwörter wird verhindert.
- Das Kennwort darf während der Anmeldung nicht offen einsehbar sein.
- Fehlerhafte Anmeldeversuche werden protokolliert und auf zehn begrenzt, danach wird das Benutzerkonto für 30 Minuten gesperrt.

Kennwörter für privilegierte Zugriffsberechtigungen

Mit der Nutzung von privilegierten Zugangsberechtigungen (z. B. Administrator-Kennungen und Fernzugängen) sind höhere Risiken bezüglich des Verlusts vertraulicher Informationen, der Verfälschung von Daten oder des Datenverlusts verbunden. Aufgrund dieser höheren Kritikalität gelten für solche Kennwörter weitergehende Anforderungen an die Komplexität und den Zugangsschutz, wie folgt:

- Passwort-Länge: mindestens 20 Zeichen
- Verwendete Zeichen: Großbuchstaben + Kleinbuchstaben + Zahlen + Sonderzeichen
- Hinterlegung eines Super-Admin-Accounts an einem gesicherten Ort und Benennung eines Zugangsberechtigten für den Notfall

Hinweise für mobile, internetfähige Geräte (z.B. Smartphones oder Tablets)

Auf Endgeräten, bei denen die Verwendung des Nutzer:innen-Accounts aus technischen Gründen nicht möglich ist, sind folgende alternative Verfahren zulässig:

- Alphanummerische Passwörter
- PINs: mindestens vierstellig, Begrenzung der Falscheingaben auf max. 5 Versuche, keine einfach einzugebenden PINs, wie 1234, 0000, 2580, 0852, 1212, oder Geburtsdaten/Jahreszahlen
- Biometrische Merkmale, wie Fingerabdruck oder Gesichtserkennung

Nicht zulässig sind unabhängig vom Anwendungsfall: (Wisch-)Muster

Pflichten der Nutzer:innen

Für den sicheren Umgang mit Zugangsdaten und Kennwörtern sind alle Nutzer:innen selbst verantwortlich.

Kennwörter sind unbedingt geheim zu halten. Sie dürfen gegenüber anderen Personen nicht offengelegt werden; auch nicht für Abwesenheiten oder zeitweilige Vertretungen. Dies gilt insbesondere für Mitglieder der Leitung und Administrator:innen.

Kennwörter, die für private Zwecke genutzt werden, dürfen nicht für dienstliche Belange benutzt werden und umgekehrt. Kennwörter, die für dienstliche Zwecke genutzt werden, dürfen nicht zusammen mit Kennwörtern für private Zwecke gespeichert werden. Beispielsweise dürfen diese nicht zusammen in einem einzelnen Passwort-Tresor gespeichert werden.

Für Studierende bietet die Viadrina ein Online-Portal an, über das im Selfservice das Kennwort geändert oder zurückgesetzt werden kann.

Bei Vergessen des Kennworts sprechen Nutzer:innen bei der IT persönlich, von der eigenen dienstlichen Telefonnummer oder im Video-Identverfahren vor, um das Kennwort zurückzusetzen. Grundsätzlich geben Nutzer:innen das neue Kennwort selbst nach den entsprechenden Qualitätsanforderungen ein.

Nur wenn dies nicht möglich ist, wird durch die IT-Beschäftigten ein temporäres Kennwort vergeben, mit dem Hinweis, dass dies unverzüglich durch die oder den Nutzer:in selbst zu ändern ist.

Falls es Anzeichen dafür gibt, dass Zugangsdaten, Kennwörter oder IT-Systeme kompromittiert sein könnten, muss dies als Sicherheitsvorfall gemeldet werden. Die betreffenden Kennwörter sind umgehend zu ändern.

Die Richtlinie tritt mit der Unterzeichnung in Kraft.

Frankfurt (Oder), 26.04.2022

LMelcher

Lisa Melcher
komm. Direktorin IKMZ