Technisch-organisatorische Maßnahmen (TOM) zur Gewährleistung und Einhaltung der Datensicherheit im AMDC

Version 1.2 | Stand 30.09.2022

Zugangsstelle

- Die Zugangsstelle muss sich in einem separaten Raum der Forschungseinrichtung befinden, in dem physische Risiken wie unbefugte Einsichtnahme und Beobachten von Tätigkeiten sowie Verlust oder Diebstahl verhindert werden. Die Zugangsstelle darf sich keinesfalls in einem offenen oder öffentlichen Raum befinden.
- Der Raum, in dem sich die Zugangsstelle befindet, muss abschließbar sein.
- Es dürfen keine Video- oder sonstigen Überwachungssysteme in dem Raum, in dem sich die Zugangsstelle befindet, installiert sein.
- Wenn der Raum nicht als Zugangsstelle genutzt wird, kann er für andere Zwecke verwendet werden. Diese Zwecke dürfen nicht im Widerspruch zur Nutzung als Zugangsstelle stehen.
- Die Reinigung oder technische Wartung des Raums darf nur erfolgen, wenn er nicht als Zugangsstelle genutzt wird.
- Die Zugangsstelle innerhalb des Raumes muss so gestaltet sein, dass keiner weiteren Person als der:dem zur Einsichtnahme befugten Forschenden eine Einsichtnahme ermöglicht wird.
- Sobald die Zugangstelle von der:dem zur Einsichtnahme befugten Forschenden – auch nur kurzfristig – verlassen wird, ist eine Einsichtnahme durch eine weitere Person durch geeignete technische Maßnahmen am Endgerät zu verhindern (z.B. VDI-Logout, Bildschirmsperre, Abdrehen des Endgerätes).

Endgerät für den Zugang

Das für den Zugang verwendete Endgerät muss von der wissenschaftlichen Einrichtung verwaltet werden und ausgestattet bzw. gesichert sein mit:

- gewartetem Betriebssystem (Windows, Linux, macOS,) mit aktuellen Software-Patches,
- nach dem Stand der Technik aktuellem Virenschutzprogramm,
- Passwort, biometrischem oder sonstigem Sicherheitsverfahren zur Inbetriebnahme,
- Webbrowser, dessen Version vom Hersteller aktuell unterstützt wird, um einen sicheren Log-In in die Virtuelle Desktop-Infrastruktur zu gewährleisten,
- stabiler Internetverbindung und
- VMware Horizon Client Software in vorgegebener Version.

Zweites, separates Endgerät für die Zwei-Faktor-Authentifizierung

Das für die Zwei-Faktor-Authentifizierung zu verwendende Endgerät (z.B. ein Smartphone) darf ausschließlich in Verwendung der:des für den Zugang berechtigten Forschenden stehen und muss ausgestattet bzw. gesichert sein mit:

- Vom Hersteller unterstützten Betriebssystem (z.B. Android oder iOS), das von der Technologie des zweiten Faktors unterstützt wird,
- Passwort, biometrischem oder sonstigem Sicherheitsverfahren zur Inbetriebnahme und
- Authentifizierungs-App in der vom Hersteller aktuell zur Verfügung gestellten Version.

Verpflichtungen

Institution

- Verwendung des Zugangs ausschließlich für ein stattgegebenes Forschungsvorhaben und nicht zu einem anderen als dem zulässigen und rechtmäßigen wissenschaftlichen Zweck.
- Zugang nur für Forschende, die mit der wissenschaftlichen Einrichtung ein aufrechtes Dienstverhältnis haben, sich schriftlich zur Einhaltung aller Geheimhaltungsverpflichtungen (insbesondere des Statistikgeheimnisses gemäß § 17 Bundesstatistikgesetz) verpflichtet haben und sich schriftlich verpflichtet haben, die für die Zwei-Faktor-Authentifizierung zugewiesenen persönlichen Zugangsdaten (Passwort und Sicherheitscode) geheim zu halten, nicht weiterzugeben und vor Einsichtnahme zu schützen.
- Bei Ausscheiden aus der wissenschaftlichen Einrichtung bzw. dem Forschungsvorhaben bzw. Wechsel einer:eines zugangsberechtigten Forschenden ist dies nachweislich bekanntzugeben.
- Belehrung aller Forschenden über Datensicherheitsmaßnahmen der Datenschutz-Grundverordnung und aller datenschutzrechtlichen Vorgaben.
- Bestellung einer:eines Datenschutzbeauftragten.

Forschende

- Einhaltung aller Datensicherheitsmaßnahmen der Datenschutz-Grundverordnung und aller datenschutzrechtlichen Vorgaben.
- Verpflichtung zur Geheimhaltung und zur absoluten Verschwiegenheit über alle zugänglich gemachten Daten.
- Verbot, die Konfiguration des zur Verfügung gestellten Statistikprogramms zur Protokollierung der Arbeitsschritte bzw. die vom jeweiligen Statistikprogramm erzeugten Protokolldateien zu ändern.
- Verbot der Ermöglichung einer Einsicht- oder Kenntnisnahme durch eine andere Person oder des Zugänglichmachens von Daten an eine andere Person als der:den Forschenden.
- Verbot der Verwendung jeglicher Funktionen einer Bildschirmaufnahme, Bildschirmfreigabe, jeglicher Videokonferenz-Tools oder sonstiger derartiger Verfahren während des Zugangs.
- Verbot des Fotografierens, Abschreibens oder Anfertigens einer Bildschirmkopie.
- Verbot, Daten auf sonst eine Weise (etwa durch die Anfertigung schriftlicher Aufzeichnungen) außerhalb der Zugangsstelle verfügbar zu machen.
- Verbot des Versuchs einer Re-Identifikation von statistischen Einheiten.
- Verbot einer gleichzeitigen Nutzung des Internets während des Zugangs für andere Zwecke.
- Verbot der Nutzung sonstigen Medien und Informationsquellen während des Zugangs.
- Im Ergebnis des Forschungsvorhabens ist der Rückschluss auf Betroffene auch im Wege einer indirekten Identifikation auszuschließen.
- Der Quellcode ist so zu erstellen, dass eine automatisierte Kontrolle der Wahrung der Geheimhaltung durch geeignete Routinen, insbesondere die Implementierung von Fallzählern, unterstützt wird.