Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Informatikdienste
Direktion

ETH Zürich
Anja Harder
IT Security Officer Informatikdienste
OCT G19
Binzmühlestrasse 130
8050 Zürich

+41 44 632 82 29
anja.harder@id.ethz.ch
www.id.ethz.ch

IT-Richtlinien und IT-Grundschutz-vorgaben der ETH Zürich

Ausgabe 2022

Inhalt

Der Vizepräsident für Infrastruktur der ETH Zürich und der Chief Information Security Officer der ETH Zürich

gestützt auf Art. 11b der «Organisationsverordnung ETH Zürich»[1], sowie auf Art. 4, Abs. 1c der «Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich» (BOT)[2] und Art. 5, Abs. 5a der Weisung «Informationssicherheit an der ETH Zürich»[3]

verordnen:

Allgemeine Bestimmungen

Artikel 1 Gegenstand

Diese Richtlinien und Vorgaben regeln:

- Aufgaben, Kompetenzen und Verantwortlichkeiten zentraler Rollen im IKT[4]-Betrieb sowie
- den Grundschutz für IKT-Mittel und
- den Umgang mit IKT-Mitteln

Sie bezwecken, dass für alle IKT-Mittel eine verantwortliche Person identifiziert ist und erreicht werden kann und dass bekannte Schwachstellen zeitgerecht beseitigt werden.

Artikel 2 Geltungsbereich und Verbindlichkeit

Diese Richtlinien sind verbindlich für die IKT-Mittel und Daten der ETH Zürich.

[1] RSETHZ 201.021
[2] RSETHZ 203.21 (BOT)
[3] RSETHZ 203.25
[4] IKT: Informations- und Telekommunikationstechnologie

Artikel 3 Begriffe

[1]*Anderswo definiert:*

Begriff	**Referenz**	**Definition**
Benutzer	BOT, Art. 2, Abs. 4	Benutzer sind alle Angehörigen der ETH Zürich (Art. 13 ETH-Gesetz) und Dritte, die zur Nutzung von IKT-Mitteln der ETH Zürich berechtigt sind (z.B. Gäste, Kongressteilnehmer, angeschlossene Organisationen, Bibliothekskunden an öffentlichen Arbeitsplätzen, Mitarbeitende von Spin-off Unternehmen der ETH Zürich oder anderen Unternehmen, sofern eine entsprechende vertragliche Vereinbarung vorliegt, emeritierte Professoren und pensionierte Mitarbeitende).
Chief Information Security Officer (CISO)	BOT, Art. 2, Abs. 12 und Weisung «Informationssicherheit an der ETH Zürich», Art. 5	Chief Information Security Officer (CISO) ist die Person, die gemäss Art. 5 Weisung Informationssicherheit an der ETH Zürich hochschulweit für die Gewährleistung der Informationssicherheit zuständig und verantwortlich ist. Sie arbeitet dafür mit den Stellen gemäss Art. 6-11 Weisung Informationssicherheit an der ETH Zürich zusammen.
Cloud Computing	ISO/IEC 17788:2014, Informationstechnik – Cloud Computing – Übersicht und Vokabular, Abs. 3.2.5	Paradigma, einen netzwerkbasierten Zugang auf ein skalierbares und elastisches Reservoir gemeinsam nutzbarer physikalischer oder virtueller Ressourcen nach dem Selbstbedienungsprinzip und bedarfsgerechter Administration zu ermöglichen. ANMERKUNG Beispiele für Ressourcen sind Server, Betriebssysteme, Netzwerke, Software, Anwendungen und Speichergeräte.
Cloud-Dienst, Cloud-Dienstleistung[5]	ISO/IEC 17788:2014, Informationstechnik – Cloud Computing – Übersicht und Vokabular, Abs. 3.2.8	Eine oder mehrere über Cloud Computing angebotene Tauglichkeiten, die mit Hilfe einer definierten Schnittstelle aufgerufen werden.
Cloud-Dienstleister	ISO/IEC 17788:2014, Informationstechnik – Cloud Computing – Übersicht und Vokabular, Abs. 3.2.15	Partei, die Cloud-Dienste bereitstellt.

[5] Der Begriff «Cloud Service» wird in diesem Dokument synonym verwendet.

Begriff	**Referenz**	**Definition**
IT-Betreiber	Weisung «Informationssicherheit an der ETH Zürich», Art. 3	Betreiber von IT-Services und -Infrastrukturen für die ETH Zürich sind namentlich die Informatikdienste, das CSCS, die Informatiksupportgruppen der Departemente (ISG).
IT Security Officer Informatikdienste (ITSO ID)	Weisung «Informationssicherheit an der ETH Zürich», Art. 8, Abs. 2	Er/Sie ist fachlich verantwortlich für die IT-Sicherheit der Services, die durch die ID für die zentralen und dezentralen Organisationseinheiten der ETH Zürich erbracht werden und diesbezüglich zentrale Ansprechpartner/in des/der CISO. Darüber hinaus berät er/sie den/die CISO und die ISOs bei Bedarf in Fragen der IT-Sicherheit.
IKT-Mittel	BOT, Art. 2, Abs. 1	IKT-Mittel (Ressourcen) umfasst alle Mittel der Informations- und Telekommunikationstechnologie, die im Eigentum der ETH Zürich sind oder im Auftrag der ETH Zürich eingesetzt werden. Es handelt sich insbesondere um Systeme, Einrichtungen und Dienste, die zur elektronischen Bearbeitung von Daten eingesetzt werden (z.B. Datenverarbeitungsanlagen, Netzwerkkomponenten, Datenspeicher, Drucker, Scanner, Telekommunikationsnetze und auf diesen Mitteln laufende Software, Schliesssysteme oder durch die ETH Zürich ausgelagerte Dienstleistungen wie Cloud-Lösungen). Ferner beinhaltet der Begriff nicht ETH Zürich-eigene Systeme (z.B. private Laptops) im Datennetz der ETH Zürich. Ausgenommen ist die Videoüberwachung gemäss ETH-Gesetz.
Mandant (en: tenant)	ISO/IEC 17788:2014, Informationstechnik – Cloud Computing – Übersicht und Vokabular, Abs. 3.2.37	Ein oder mehrere Cloud-Dienstleistungsnutzer die sich den Zugriff auf eine Menge physikalischer und virtueller Ressourcen teilen.
Organisationseinheiten	BOT, Art. 2, Abs. 6	Organisationseinheiten sind von der Schulleitung gemäss Organisationsverordnung ETH Zürich (OV) vom 16.12.2003 errichtete zentrale oder dezentrale Organe der ETH Zürich (z.B. Departemente, Institute, Abteilungen, Stabsstellen, selbständige Professuren) sowie Lehr- und Forschungseinrichtungen ausserhalb der Departemente gemäss Art. 61.

Begriff	**Referenz**	**Definition**
Service-Vermittelnde, System- und Netzwerkzonen-verantwortliche	BOT, Art. 2, Abs. 11	sind die in den *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* und in Artikel 6 dieses Erlasses definierten Fachpersonen.
Streng vertraulich	Weisung «Informationssicherheit an der ETH Zürich», Art. 22, Abs. 1	Als «streng vertraulich» gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich schwerwiegend beeinträchtigen kann.
Vertraulich	Weisung «Informationssicherheit an der ETH Zürich», Art. 22, Abs. 1	Als «vertraulich» gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich erheblich beeinträchtigen kann.

[2] *Externer IKT-Service*:

Von der ETH Zürich bezogene IKT-Dienstleistung, die ausserhalb des Netzwerks der ETH Zürich von einer Fremdfirma erbracht wird (z.B. Cloud-Dienstleistung).

[3] Fernzugang:

Zugang zu IKT-Mitteln von ausserhalb des Datennetzes der ETH Zürich (remote access).

Rollen

Artikel 4 Netzwerkzonenverantwortliche

[1] Verantwortlichkeiten

Zusätzlich zu den in der BOT erwähnten Vorgaben, sind sie verantwortlich für die Sicherheit ihrer Zonen und die dazugehörigen Prozesse, insbesondere für die Einhaltung der im jeweiligen Kontext anwendbaren IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich.

[2] Aufgaben

a) Teilnahme an der von den Informatikdiensten angebotenen Ausbildung für Netzwerkzonenverantwortliche.

b) Dokumentation der Einsatzzwecke der ihnen zugeteilten Netzwerkzonen.

c) Kenntnis und Umsetzung der anwendbaren IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich.

d) Erstbeurteilung von Ausnahmeanträgen zu IKT-Mitteln in seiner/ihrer Netzwerkzone, sowie die Weiterleitung der von ihm/ihr unterstützten Anträge an die/den IT Security Officer Informatikdienste.

e) Netzwerkzonenverantwortliche müssen für jedes IT-System in ihren Zonen die Systemverantwortlichen benennen oder zeitnah herausfinden können.

[3] Kompetenzen

a) Festlegen der Einsatzzwecke der ihnen zugeteilten Netzwerkzonen. Der Einsatzzweck einer Netzwerkzone muss mit dem Typ der bei den Informatikdiensten beantragten Netzwerkzone korrespondieren (z.B. DMZ, IoT, BYOD).

b) Entscheidung, welche IKT-Mittel sich in ihre Zonen verbinden dürfen, wobei als Rahmenbedingung dem Typ der Netzwerkzone entsprochen werden soll.

c) Entscheid über Änderungsanträge bezüglich der Konfigurationen ihrer Zonenfirewalls gemäss Art. 9, Abs.5 dieser Verordnung.

d) Ablehnung von Ausnahmeanträgen[6], die sich auf IKT-Mittel in Netzwerkzonen ihrer Zuständigkeit beziehen.

e) Beantragen von Ausnahmen bezüglich der Einhaltung von IT-Richtlinien und IT-Grundschutzvorgaben.

[4] Ernennung

Die Organisationen nehmen die Netzwerkzonenverantwortung, inkl. der Verantwortung für allfällige Zonenfirewalls, selbst wahr oder delegieren sie an ausschliesslich ETH Zürich-interne Dienstleister. Voraussetzung dafür ist der Abschluss eines schriftlichen Service Level Agreements (SLA), in welchem die zu erbringenden Leistungen sowie die mit der Netzwerkzonenverantwortung einhergehenden und umzusetzenden IT-Grundschutzvorgaben

[6] Rahmenbedingungen für Ausnahmebewilligungen sind in Art. 12 geregelt.

geregelt sind. Im Falle einer Delegation bleiben die Organisationseinheiten insbesondere für die Auftragserteilung und die Kontrolle der SLA-Einhaltung verantwortlich[7].

[5] Meldung

a) Die Organisationseinheiten melden die Netzwerkzonenverantwortlichen an die Informatikdienste.

b) Wird eine Zone durch eine Firewall geschützt, muss zusätzlich zum Netzwerkzonenverantwortlichen mindestens eine, maximal drei Stellvertretungen gemeldet werden.

Artikel 5 Systemverantwortliche

[1] Verantwortlichkeiten

Zusätzlich zu den in der BOT erwähnten Vorgaben, sind sie verantwortlich für die Systempflege und dabei insbesondere für die Einhaltung der im jeweiligen Kontext relevanten IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich.

[2] Aufgaben

a) System- und Systemsicherheitspflege

b) Umsetzung der anwendbaren IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich.

[3] Kompetenzen

Beantragen von Ausnahmen[8] bezüglich der Einhaltung von IT-Richtlinien und IT-Grundschutzvorgaben.

[4] Ernennung

a) IKT-Mittel im Eigentum der ETH Zürich:

Die Organisationseinheiten nehmen die Systemverantwortung selbst wahr oder delegieren sie an einen Dienstleister[9]. Voraussetzung für eine Delegation ist der Abschluss eines schriftlichen Service Level Agreements (SLA), in welchem die zu erbringenden Leistungen sowie die mit der Systemverantwortung einhergehenden und umzusetzenden IT-Grundschutzvorgaben geregelt sind. Im Falle einer Delegation der Systemverantwortung bleiben die Organisationseinheiten insbesondere für die Auftragserteilung und die Kontrolle der SLA-Einhaltung verantwortlich.[10]

b) Nicht ETH Zürich-eigene IKT-Mittel im Netzwerk der ETH Zürich:

Bei nicht ETH Zürich-eigenen IT-Systemen im Netzwerk der ETH Zürich, wie beispielsweise private IT-Systeme von Studierenden oder IT-Systeme Dritter, gilt der/die

[7] Accountable im Sinne der RACI-Notation
[8] Rahmenbedingungen für Ausnahmebewilligungen sind in Art. 12 geregelt.
[9] z.B. Informatikdienste
[10] Accountable im Sinne der RACI-Notation

angemeldete Benutzer/in als Systemverantwortliche/r, sofern kein Systemverantwortlicher oder keine Systemverantwortliche gemeldet ist[11].[12]

[5] Meldung

a) Die Organisationseinheiten melden die von ihnen ernannten Systemverantwortlichen und deren Stellvertretungen an die Informatikdienste.

b) Falls die Zuordnung einer systemverantwortlichen Person bei den Informatikdiensten nicht hinterlegt ist, wird diese Information nach Möglichkeit aus den vorhandenen Informationen (wie Logs oder Systemzustände) abgeleitet.

Artikel 6 Service-Vermittelnde

[1] Beschreibung

Service-Vermittelnde beziehen externe IT-Dienstleistungen (z.B. Cloud-Dienstleistungen) und stellen diese Dienste Angehörigen der ETH Zürich zur Verfügung. Service-Vermittelnde können einerseits IT-Betreiber oder aber auch technisch-administrative oder wissenschaftliche Mitarbeitende der Departemente und der zentralen Organe der ETH Zürich sein (z.B. Professor/innen, Departementskoordinator/innen, Abteilungsleiter/innen). Benutzende, die einen externen IKT-Service ausschliesslich für sich selbst beziehen, gelten nicht als Service-Vermittelnde.

[2] Verantwortlichkeiten

Service-Vermittelnde sind innerhalb der ETH Zürich verantwortlich für Angelegenheiten im Zusammenhang mit der Nutzung und Verwaltung von einem oder mehreren externen IKT-Services, die durch Angehörige der ETH Zürich im Auftrag der ETH Zürich genutzt werden (Cloud Dienstleitungen etc.). Dabei verantworten sie insbesondere das Vertragsmanagement, die Vereinbarung der im jeweiligen Kontext relevanten IT-Richtlinien und IT-Grundschutz-vorgaben, die Kontrolle von deren Einhaltung und die Freigabe des Services für bestimmte Einsatzzwecke.

[3] Aufgaben

a) Durchführen einer Risikobeurteilung, um die Eignung des externen IKT-Services für den vorgesehenen Einsatzzweck zu beurteilen.

b) Sicherstellen, dass die IT-Richtlinien und IT-Grundschutzvorgaben umgesetzt werden können. Vertragsrelevante Vorgaben sollen mit dem Service-Anbieter verbindlich vereinbart werden.

c) Sicherstellen, dass die ETH Zürich über Änderungen, Störungen oder Vorfälle informiert bzw. konsultiert wird und dass die relevanten Informationen an die betroffenen Benutzenden weitergeben werden.

[11] BOT, Art. 6, Abs. 6

[12] Beispiele für Systeme Dritter sind: Laptop oder Smartphone einer Beratungsfirma. Die Firma hat im Rahmen ihrer vertraglichen Beziehung zur ETH Zürich die Verantwortung für das System

d) Absprache mit dem IT-Security Center der Informatikdienste bzgl. der Notwendigkeit einer Sicherheitsüberwachung des externen IKT-Services. Bei Bedarf zeitnahe Lieferung der dafür benötigten unveränderten Log-Daten an das IT-Security Center.

e) Kontrolle der Einhaltung des Service Level Agreements und bei Bedarf einfordern notwendiger Verbesserungen beim Service-Anbieter.

f) Bei Bedarf Festlegen und Umsetzung von ergänzenden technischen oder organisatorischen Massnahmen zur Absicherung des externen IKT-Services.[13]

g) Bereitstellen der Dokumentation für Benutzende. Diese erläutert Einsatzzweck und Nutzungsumfang des Services, die mitgeltenden Nutzungsbedingungen, wie beispielsweise die Freigabe oder das Verbot der Bearbeitung von vertraulichen Informationen mit dem externen IKT-Service.

h) Periodisch prüfen, ob und wie die Daten der ETH Zürich bei einem möglichen Nutzungsende des externen IKT-Services in IKT-Services der ETH Zürich migriert werden können.

i) Sicherstellen, bei Nutzungsende des externen IKT-Services die Daten der ETH Zürich in IKT-Services der ETH Zürich migriert werden können.

[4] Kompetenzen

a) Entscheid über Einsatzzweck und Nutzungsumfang des externen IKT-Services und der für die Angehörigen der ETH Zürich geltenden Nutzungsbedingungen.

b) Beantragen von Ausnahmen[14] bezüglich der Einhaltung von IT-Richtlinien und IT-Grundschutzvorgaben.

[5] Ernennung

Die Organisationseinheiten, die die Nutzung von Cloud-Lösungen oder anderen externen IKT-Services in Auftrag geben, ernennen dafür eine/n oder mehrere ETH-interne/n Verantwortliche/n. Vorzugsweise wird die Rolle «Service-Vermittelnde/r» für externe IKT-Services auf Ebene Departement, Institut oder Abteilung zentralisiert.

[6] Delegation von Aufgaben

Die Aufgaben des/der Service-Vermittelnden können delegiert werden, die Verantwortung verbleibt bei dem/der Verantwortlichen.

[7] Meldung

Die Organisationseinheiten melden den externen IKT-Service, dessen Einsatzzweck und Nutzungsumfang und die von ihnen ernannten Verantwortlichen und deren Stellvertretungen an die Informatikdienste.

[13] z.B. Backup, Logging, Reporting.
[14] Rahmenbedingungen für Ausnahmebewilligungen sind in Art. 12 geregelt.

Artikel 7 Erreichbarkeit der Verantwortlichen

Systemverantwortliche, Netzwerkzonenverantwortliche, Service-Vermittelnde und deren Stellvertretungen müssen über von den Informatikdiensten vorgegebene E-Mail-Adressen erreichbar sein und innerhalb eines Arbeitstages auf Meldungen und Anfragen bezüglich möglicher IT-Sicherheitsvorfälle reagieren.

IT-Grundschutz

Artikel 8 IT-Grundschutzvorgaben für Benutzende

[1] Grundsatz der Nutzung von internen und externen IKT-Services der ETH Zürich

a) Grundsätzlich sind zur Datenbearbeitung und Speicherung die ETH-internen oder externen IKT-Services zu nutzen, die von den IT-Betreibern der ETH Zürich, respektive von den IT-verantwortlichen Personen der Institute und Professuren angeboten oder zugelassen[15] werden. Dabei sind die Nutzungsbedingungen für die jeweiligen Services einzuhalten.

b) Für Ausnahmen von diesem Grundsatz, beispielsweise, wenn im Rahmen von Kooperationen Daten der ETH Zürich auf Kollaborationsplattformen oder Speicherservices externer Kooperationspartner[16] oder Dritter bearbeitet oder abgelegt werden sollen, ist vorgängig die Zustimmung der zuständigen Linie, Forschungs- oder Projektleitung der ETH Zürich einzuholen. Die Kontrolle (z.B. Zugriff, Schutzlevel) über solche Datenbestände muss für die ETH Zürich jederzeit gewährleistet sein und verbindlich geregelt werden. Das gilt insbesondere auch für Fälle, in denen Benutzende aufgrund aussergewöhnlicher Ereignisse (Krankheit, Todesfall etc.) über einen längeren Zeitraum nicht auf die Daten zugreifen können.

c) Die Nutzung von externen IKT-Services zur Unterstützung im Tagesgeschäft (z.B. Online-Übersetzungsservices), die nicht von der ETH Zürich angeboten werden, liegt in der Verantwortung des/der Benutzenden. Vertrauliche Daten, streng vertrauliche Daten oder Personendaten dürfen mit solchen Services nicht bearbeitet werden.

[2] Externe Speicherung oder Bearbeitung vertraulicher Daten

a) Grundsätzlich darf ein externer IKT-Service (z.B. Cloud-Dienstleistung) für die Bearbeitung und Speicherung von vertraulichen Daten genutzt werden, sofern er durch die/den zuständige/n Service-Vermittelnde/n für die Nutzung mit vertraulichen Daten freigegeben wurde.

b) Einschränkend gilt, dass ein/e Informationseigner/in die Bearbeitung und Ablage eines Informationsbestands in der Cloud untersagen[17] kann. Im Zweifelsfall ist der/die Informationseigner/in zu kontaktieren.

[15] z.B. selbstverwaltete Systeme im Eigentum der ETH Zürich oder Systeme, die nicht im Eigentum der ETH Zürich sind (z.B. «Bring Your Own Device»)
[16] z.B. mit anderen Universitäten oder Industriepartnern
[17] Weisung Informationssicherheit, Anhang 2, «Elektronische Informationen in der Cloud» RSETHZ 203.25

[3] Softwareaktualisierungen

a) Erhalten Benutzende IT-sicherheitsrelevante Aktualisierungen von Systemsoftware und Anwendungen (Patches und Updates), müssen sie diese schnellstmöglich, spätestens innerhalb von zwei Arbeitstagen nach Verteilung durch den zuständigen IT-Support, installiert und bei Bedarf durch einen Neustart des IT-Systems aktiviert werden. Kurze Verlängerungen dieser Frist sind in Absprache mit dem zuständigen Systemverantwortlichen möglich.

b) Bei geplanter Abwesenheit der/des zuständigen Benutzenden muss das IT-System heruntergefahren oder vom Netzwerk getrennt werden. Nach der Rückkehr ist es unmittelbar zu aktualisieren. IT-Systeme, die trotz Abwesenheit der zuständigen Benutzenden nicht heruntergefahren werden, müssen durch eine Stellvertretung betreut werden.

[4] Sicherheitsfunktionen nicht deaktivieren

Von den Systemverantwortlichen implementierte Sicherheitsmassnahmen, wie beispielsweise Virenschutzprogramme oder Programme zur Identifikation von Sicherheitsschwachstellen, lokale Firewalls oder Sicherheitseinstellungen, dürfen nur in Absprache mit dem/der Systemverantwortlichen, respektive dem/der Service-Vermittelnden geändert werden.

[5] Verschlüsselung mobiler Datenträger

Mobile Datenträger, auf denen als «vertraulich» oder «streng vertraulich» klassifizierte Daten[18] abgelegt sind, müssen verschlüsselt und mit einem sicheren Passwort oder anderen Authentisierungsmitteln geschützt werden.

[6] Bildschirmsperre

Unbefugter Zugang zu unbeaufsichtigten IT-Systemen muss durch eine zugangsgeschützte Bildschirmsperre verhindert werden, sofern Benutzende sich nicht vollständig vom IT-System abmelden.

[7] Umgang mit Authentisierungsmitteln

a) Authentisierungsmittel wie Passwörter, PINs, Private Keys, Chipkarten und andere physische Token sind persönlich und als «streng vertraulich» klassifiziert. Sie dürfen anderen Personen nicht offengelegt oder weitergegeben werden.

b) Ist das Teilen eines Benutzungskontos[19] und des zugehörigen Passworts aus technischen Gründen zwingend, darf das Passwort an die berechtigten Personen weitergegeben werden.

c) Werden Passwörter oder PINs niedergeschrieben, müssen sie geschützt aufbewahrt werden, so dass Unbefugte keine Einsicht erhalten können.

d) Die elektronische Speicherung von Authentisierungsmitteln muss mit aktuell als hinreichend sicher geltenden Mitteln verschlüsselt erfolgen. Das Passwort zum Öffnen

[18] Definition der Vertraulichkeitsstufen Weisung Informationssicherheit, Art. 22, RSETHZ 203.25
[19] «shared account»

der Ablage muss mindestens den Passwortregeln der ETH Zürich[20] entsprechen und sich von jedem anderen Passwort des/der betreffenden Benutzenden unterscheiden. Sofern möglich, soll die elektronische Ablage mit Multifaktorauthentisierung geschützt werden.

[8] Passwörter und PINs

Die Passwort- und PIN-Regeln gemäss Anhang dieses Dokuments müssen eingehalten werden.

[9] Systemverantwortung für selbstverwaltete Systeme

Benutzende von selbstverwalteten Systemen[21] nehmen die Rolle der Systemverantwortlichen wahr und müssen entsprechend auch Art. 10 einhalten.

Artikel 9 IT-Grundschutzvorgaben für Netzwerkzonenverantwortliche

[1] Mit einer Zone des Netzwerkes der ETH Zürich dürfen nur die IT-Systeme verbunden werden, die deren Einsatzzweck entsprechen. Nach Möglichkeit sollen IT-Systeme mit gleichem Schutzbedarf in eigenen Zonen oder Teilbereichen von Zonen geschützt werden.

[2] Enthält eine Zone IT-Systeme, bei denen die IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich länger als 20 Tage nicht eingehalten werden, ist die Zone so zu isolieren, dass allfällige Schwachstellen von ausserhalb der Zone nicht ausnutzbar sind. Alternativ können die betroffenen Systeme in eine bereits isolierte Zone verschoben werden.

[3] Für alle IP-Adressen in einer Zone sind die zuständigen Systemverantwortlichen den Netzwerkzonenverantwortlichen bekannt oder können kurzfristig herausgefunden werden.

[4] Die Nutzung der limitiert vorhandenen IP-Adressen ist restriktiv zu halten. Ungenutzte IP-Adressen müssen den Informatikdiensten zurückgegeben werden. Die Nutzung und der Verbrauch von IP-Adressen muss regelmässig überprüft werden (DHCP-Fixierungen).

[5] Zonenfirewalls sind grundsätzlich geschlossen. Ports und/oder Protokolle werden durch die Informatikdienste nur mit Bewilligung des/der Netzwerkzonenverantwortlichen geöffnet. Der/die Netzwerkzonenverantwortliche führt vorgängig eine Risikoeinschätzung hinsichtlich der Stabilität und Verwundbarkeit des Netzwerks, sowie unter Berücksichtigung des Schutzbedarfs der Datenbestände durch. Die Informatikdienste verfügen über ein Vetorecht bzgl. der Umsetzung von Änderungen, die die Stabilität des Netzwerks beeinträchtigen oder Verwundbarkeiten des Netzes oder der IKT-Mittel verursachen könnten.

[6] Aktivierungen, Änderungen und Deaktivierungen von Firewall-Regeln müssen nachvollziehbar erfolgen. Für jede Firewall-Regel ist der/die Antragsteller/in, der/die Nutzende, der Zweck/die Funktionalität zu dokumentieren. Ebenfalls müssen der/die Ausführende sowie der Zeitpunkt der Aktivierung und Deaktivierung dokumentiert sein.

[20] siehe Anhang zu diesem Dokument: Passwort- und PIN-Regeln der ETH Zürich
[21] «self-managed»-Systeme der ETH Zürich oder BYOD

[7] Firewall-Regeln müssen halbjährlich überprüft und aktualisiert werden. Nicht mehr benötigte Regeln sind zu entfernen.

[8] Firewall-Logs müssen durch die Netzwerkzonenverantwortlichen periodisch auf Unregelmässigkeiten überprüft werden.

[9] Benutzende und IT-Systeme müssen sich über NAC-Technologien authentisieren resp. autorisieren, um in eine Zone verbunden zu werden. Die Liste an zugelassenen Benutzenden (Realms) und IT-Systemen (Zertifikate, MAC-Adressen) wird regelmässig überprüft. Authentisierungs- und Autorisierungs-Logs werden periodisch durch die Netzwerkzonenverantwortlichen auf Unregelmässigkeiten überprüft (RADIUS).

[10] Jedes IT-System muss einen Eintrag im DNS (Domain Name System) der Informatikdienste haben. Die DNS-Konfigurationen einer Zone müssen regelmässig überprüft und aktualisiert werden.

[11] Physische Sicherheit:
Netzwerkanschlüsse müssen mit NAC-Methoden (Netzwerk Access Control) vor Fremdzugriffen geschützt werden. Netzwerkanschlüsse, die nicht mit NAC geschützt sind, dürfen sich ausschliesslich in geschlossenen Räumen befinden, in die nur berechtige Personen Zutritt haben.

Artikel 10 IT-Grundschutzvorgaben für Systemverantwortliche

[1] Aktualität der Software

a) Firmware, Betriebssysteme, Applikationen, Apps und andere Software muss in aktuellen, vom Hersteller unterstützten Versionen eingesetzt und bezüglich Sicherheits-aktualisierungen auf neuestem Stand gehalten werden.

b) Sicherheitsaktualisierungen müssen unmittelbar nach dem Erscheinen getestet und schnellstmöglich auf die IT-Systeme verteilt werden. Sofern die Tests keine betrieblichen Probleme aufzeigen und die betrieblichen Risiken im Vergleich zum Sicherheitsgewinn nicht unverhältnismässig gross sind, müssen die Aktualisierungen spätestens nach zehn Kalendertagen ab ihrem Erscheinungsdatum auf die Zielsysteme verteilt werden.

c) In Notfällen, bei besonderer Dringlichkeit, können der/die IT Security Officer der Informatikdienste oder die zuständigen IT-Betreiber eine unmittelbare Verteilung und Installation von Sicherheitsaktualisierungen anordnen.

d) In IKT-Umgebungen, wo dies möglich und betrieblich vertretbar ist, sollen die Installation der Aktualisierungen und ein allfälliger Neustart auf den Zielsystemen spätestens zwei Arbeitstage nach der Verteilung mit technischen Mitteln durchgesetzt werden.

[2] Schutz vor Schadprogrammen

a) Sofern verfügbar und nutzbringend, müssen IT-Systeme mit Malware-Scannern betrieben werden.

b) Die Schutzprogramme müssen aktuell sein bzgl. Software-Version, Updates und Schutzsignaturen.

c) Die Schutzprogramme sind so zu konfigurieren, dass Dateien automatisch bei Zugriff geprüft werden.

d) Zur Laufzeit eines IT-Systems muss automatisch, nach Möglichkeit mindestens stündlich, nach Aktualisierungen gesucht werden und diese müssen automatisch eingespielt werden.

[3] Verschlüsselung von Speichermedien

Sofern möglich, sind Speichermedien von Desktops und mobilen Geräten wie Laptops, Tablets, Smartphones nach jeweiligem Hersteller-Standard vollständig zu verschlüsseln.

[4] Bildschirmsperre

IT-Systeme für Endbenutzende (Desktops, Laptops, Tablets, etc.) und Server sind so zu konfigurieren, dass spätestens nach 10 Minuten Inaktivität des/der Benutzenden automatisch eine Bildschirmsperre aktiviert wird, die sich nur durch Eingabe eines Passwords, PINs, Fingerabdrucks oder mittels ähnlichen Authentisierungsmethoden freischalten lässt.

[5] Zugangskontrolle

a) Der Zugang zu Konten mit erhöhten Zugriffsrechten, wie beispielsweise «admin» oder «root», oder zu Gruppen mit Administrationsprivilegien, wie z.B. «Administratoren» oder «sudoers», muss auf möglichst wenige, für die jeweilige Rolle autorisierte Personen beschränkt werden.[22]

b) Zugriffsrechte von Benutzungskonten mit Systemadministrationsrechten müssen auf das notwendige Minimum[23] eingeschränkt und regelmässig überprüft werden.

c) Zugriffsrechte auf vertrauliche oder streng vertrauliche Datenbestände oder auf IKT-Mittel mit hohem Schutzbedarf bzgl. Integrität oder Verfügbarkeit müssen auf das notwendige Minimum[24] eingeschränkt und regelmässig überprüft werden.

d) Geteilte Benutzungskonten[25] sind nur gestattet, wenn es eine zwingende Notwendigkeit für sie gibt. Zugriffe auf geteilte Benutzungskonten müssen auf das notwendige Minimum eingeschränkt und regelmässig überprüft werden.

e) Vorkonfigurierte Benutzungskonten, wie beispielsweise «guest», müssen gelöscht werden. Falls das nicht möglich ist, müssen sie deaktiviert bzw. für eine Anmeldung gesperrt werden. Das voreingestellte Passwort muss gewechselt werden.

[22] Need-to-Know
[23] Least Privilege
[24] Need-to-Know
[25] «shared accounts»

[6] Passwort- und PIN-Policies

Sofern technisch möglich, müssen die Passwort- und PIN-Regeln der ETH Zürich[26] mittels Konfiguration von einschlägigen «Policies» z.B. im IAM, Active Directory oder auf den lokalen IT-Systemen durchgesetzt werden.

[7] Datensicherung

a) Die Datensicherung muss geregelt und im Service Level Agreement oder anderweitig dokumentiert sein.

b) Die Wiederherstellbarkeit von Backups muss periodisch stichprobenartig geprüft werden.

[8] Fernzugang (Remote Access)

a) Fernzugänge dürfen nur mit aktuell als sicher geltenden verschlüsselten Protokollen erfolgen.

b) Wenn VPN (Virtual Private Network) als Zugangstechnologie verwendet wird, muss der Zugang auf dem VPN-Endpunkt der Informatikdienste terminieren.

c) Kommen andere Fernzugangsmethoden (wie «Jump Hosts», SCION, Protokoll-Tunneling, Proxy-Technologien) zum Einsatz, müssen die Zugangslogs permanent bezüglich Anomalien (z.B. fehlgeschlagene Anmeldeversuche, Cyber-Angriffe) überwacht werden.

d) Auf Fernzugänge zugreifende IT-Systeme müssen mindestens den Sicherheitsstand aufweisen, der in diesen IT-Richtlinien und IT-Grundschutzvorgaben gefordert ist.

[9] Physische Sicherheit

Unbefugte dürfen keinen Zutritt zu IKT-Mitteln erhalten. Die notwendigen Sicherheitsmassnahmen sind an die räumlichen Gegebenheiten anzupassen. Dabei gelten die für die jeweilige Organisationseinheit anwendbaren Vorgaben zur physischen Sicherheit, wie beispielsweise das Raumkonzept[27] der Informatikdienste.

[10] Nachvollziehbarkeit

Betriebs- und sicherheitsrelevante Systemnutzungen und Systemaktivitäten, sowie Veränderungen an Systemkonfigurationen, müssen protokolliert werden.

[26] siehe Anhang zu diesem Dokument: Passwort- und PIN-Regeln der ETH Zürich
[27] Raumkonzept der Informatikdienste: https://sherlock.sp.ethz.ch/221b/policies/VPPR%20readonly%20Lib/2019_01_RL_Raum_Konzept_ID.pdf, auf Anfrage einsehbar.

Artikel 11 IT-Grundschutzvorgaben für Service-Vermittelnde

Ergänzend zu Art. 10 dieser Verordnung gelten für externe IKT-Services, die durch die ETH Zürich genutzt werden, die folgenden Vorgaben, sofern sie im jeweiligen Kontext relevant sind.

[1] Der Vertrag, das Service Level Agreement, respektive die AGB regeln insbesondere:

a) Gerichtsstand und anwendbares Recht. Aus Gründen der Rechtsdurchsetzbarkeit gilt folgende Präferenz: 1. Schweiz, 2. EU, 3. Andere.

b) Personendaten werden in der Schweiz oder der EU verarbeitet und gespeichert. Personendaten dürfen mit angemessenem vertraglichem Schutz auch im übrigen Ausland, einschliesslich Ländern mit ungenügendem Datenschutzniveau gemäss Staatenliste des Eidg. Datenschutzbeauftragten (EDÖB), bearbeitet, z.B. verarbeitet oder gespeichert werden. Bei ungenügendem Datenschutzniveau im Speicher-/Verarbeitungsland sind Personendaten von Gesetzes wegen durch die Vereinbarung von Standard Contractual Clauses (SCC) oder vergleichbare vertragliche Massnahmen zu schützen.

c) Der Service-Anbieter bestätigt, dass er die für die ETH Zürich im Kontext der Anwendung relevanten Gesetze und Verordnungen einhält[28].

d) Alle Zuständigkeiten sind eindeutig einer Partei zugeordnet.

e) Der externe Service-Anbieter verpflichtet sich zu regelmässigen unabhängigen Prüfungen der IT-Sicherheit (Audits, Zertifizierungen) und stellt Audit-Berichte zur Verfügung oder gewährt der ETH Zürich ein Prüfrecht.

f) Gegenseitige Ansprechpersonen und garantierte Reaktionszeiten, sowie die zu verwendenden Kommunikationskanäle sind geregelt, so dass bei betrieblichen Störungen oder Sicherheitsvorfällen zuverlässig und schnell reagiert werden kann.

g) Die Trennung von Daten der «ETH Zürich» von Daten anderer Kundinnen und vom administrativen Bereich des Service-Anbieters muss sichergestellt sein (Mandantenfähigkeit).

h) Die Regelung der Service-Kündigung muss die Übernahme der Daten der ETH Zürich und der Nutzungsprotokolle (Logs) durch die ETH Zürich und das Löschen dieser Daten auf Seiten des Service-Anbieters festlegen.

[2] *aufgehoben*

[3] Eine Freigabe zur Bearbeitung von *internen* Daten darf erfolgen, wenn die folgenden Bedingungen erfüllt sind:

a) Benutzende und Administratoren der ETH Zürich und des externen Service-Anbieters arbeiten mit persönlichen Benutzungskonten und authentisieren sich mit mindestens einem Faktor (z.B. Passwort).

b) Daten sind im Transport und in der Ablage verschlüsselt, jeweils mit nach aktuellem Stand der Technik als sicher geltenden Methoden.

[28] z.B. die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu) (abgerufen am 1.7.2022)

c) Aktivitäten von Benutzenden und von Administrator/innen der ETH Zürich sollen nachvollziehbar sein. Die Logs sollen für mindestens ein Jahr verfügbar sein und müssen, entsprechend den Vorgaben aus der BOT[29], spätestens nach zwei Jahren unwiederbringlich gelöscht werden.

d) Eine Schnittstelle zur zeitnahen Übernahme[30] von Logdaten über die Aktivitäten von Benutzenden und Administrator/innen der ETH Zürich durch die ETH Zürich steht zur Verfügung. Ist dies nicht möglich oder im jeweiligen Kontext nicht sinnvoll, sollen verantwortliche Stellen der ETH Zürich anderweitig auf diese Informationen zugreifen können, z.B. über entsprechende Programmschnittstellen (APIs) oder online-Verwaltungsfunktionen (Dashboards) des Services.

e) Aktivitäten des Service-Anbieters, bei denen auf Daten der ETH Zürich zugegriffen wird, müssen durch den Service-Anbieter aufgezeichnet und sollen für mindestens zwei Jahre aufbewahrt werden.

f) Die Verfügbarkeit der Daten der ETH Zürich muss entsprechend der Anforderungen der ETH Zürich sichergestellt sein. Vorzugsweise wird das durch ein regelmässiges Backup aller Daten gewährleistet, dessen Funktionsweise periodisch überprüft wird.

g) Die ETH Zürich muss Zugriff auf ihre Daten haben. Dies muss auch für Fälle sichergestellt sein, in denen Benutzende aufgrund ausserordentlicher Ereignisse über einen längeren Zeitraum nicht auf die Daten zugreifen können (Krankheit, Todesfall etc.). Im Minimum sollen der/die Service-Vermittelnde oder eine IT-Administrator/in und deren Stellvertretungen im Bedarfsfall auf die Daten zugreifen können.

h) Eine Rückführung der Daten der ETH Zürich auf IKT-Services der ETH Zürich muss bei Bedarf möglich sein.

[4] Eine Freigabe zur Bearbeitung von v*ertraulichen* Daten darf erfolgen, wenn die Bedingungen zur Bearbeitung von internen Daten und zusätzlich die folgenden Vorgaben erfüllt sind:

a) Administratoren des externen Service-Anbieters, die auf Daten und Services der ETH Zürich zugreifen, setzen für diese Zugriffe Multifaktorauthentisierung ein.

b) Benutzende und Administratoren der ETH Zürich authentifizieren sich mit Multifaktorauthentisierung.

c) Der Anbieter der Dienstleistung verwendet den Schlüssel für die Ablageverschlüsselung exklusiv für die ETH Zürich. Für Daten anderer Kunden werden andere Schlüssel eingesetzt.[31]

d) Die Verwaltung von Benutzungskonten und Zugriffsrechten erfolgt zentral durch eine ETH-interne Stelle. Eine Anbindung an die von den Informatikdiensten betriebenen Identitätsverwaltungs- und Föderationsdienste[32] soll umgesetzt werden, sofern das möglich und im jeweiligen Kontext sinnvoll ist.

[29] RSETHZ 203.21, Anhang, Ziffer 1, Nr. 3b
[30] «near realtime»
[31] Der Service-Anbieter verwendet für unterschiedliche Kunden / Tenants unterschiedliche Schlüssel.
[32] z.B. ADFS, DirX

e) Benutzenden oder Gruppen von Benutzenden müssen granulare Zugriffsrechte[33] auf einzelne Datenbestände vergeben werden können.

[5] Eine Freigabe für die Speicherung oder Bearbeitung von *streng vertraulichen* Daten ist nicht gestattet.

[6] Aktualität der Software

a) Sofern im jeweiligen Kontext anwendbar, ist punktuell zu kontrollieren, ob der Service-Anbieter Sicherheitsaktualisierungen innerhalb der vereinbarten Fristen einspielt. Verstösse gegen das Service Level Agreement sind mit dem Service-Anbieter zu thematisieren und bei wiederholten Verstössen abzumahnen.

b) Liegt die Zuständigkeit für das Einspielen von Sicherheitsaktualisierungen bei der ETH Zürich, ist wie in Art. 10 dieser Verordnung zu verfahren.

Artikel 12 Ausnahmen zu den vorgenannten Bestimmungen

[1] Externe IKT-Services

Für externe IKT-Services, für welche die im jeweiligen Kontext anzuwendenden IT-Richtlinien und IT-Grundschutzvorgaben nicht eingehalten werden können, müssen Ausnahmebewilligungen beim CISO eingeholt werden.

[2] IKT-Mittel im Netzwerk der ETH Zürich

a) IT-Systeme, bei denen Vorgaben dieser Verordnung nicht eingehalten werden können, sind in abgeschotteten Zonen des Netzwerks der ETH Zürich zu platzieren. Allfällige Schwachstellen dürfen von ausserhalb der abgeschotteten Zonen nicht ausnutzbar sein.

b) Für IT-Systeme, die in einer nicht abgeschotteten Zone betrieben werden sollen, obwohl IT-Richtlinien und IT-Grundschutzvorgaben länger als 10 Arbeitstage nicht eingehalten werden, müssen Ausnahmebewilligungen eingeholt werden.

c) Die Informatikdienste führen den Ausnahmeprozess im Auftrag des Chief Information Security Officers der ETH Zürich.

d) Für den Bewilligungsprozess gilt:

- Antragsstellung durch die/den Systemverantwortliche/n:

  Es erfolgt eine Erstbeurteilung durch die/den zuständige/n Netzwerkzonenverant-wortliche/n: Sie/er leitet die von ihm/ihr unterstützten Anträge an die/den IT Security Officer Informatikdienste weiter.

- Antragstellung durch die/den Netzwerkzonenverantwortliche/n:

  Der Antrag wird direkt an die/den IT Security Officer Informatikdienste gestellt.

[33] z.B. Erzeugen, Lesen, Verändern, Löschen

- Entscheid durch die/den IT Security Officer Informatikdienste:

  Sie/er ist verantwortlich für die Beurteilung und Bewilligung, bzw. Ablehnung von Ausnahmeanträgen.

- Eskalationen an die/den Chief Information Security Officer (CISO) der ETH Zürich:

  Sie/er ist Eskalationsstelle im Konfliktfall. Darüber hinaus ist er/sie berechtigt, das Inventar der Ausnahmeanträge (siehe Abs. 3 dieses Artikels) zu überprüfen.

- Inventarisierung:

  Die/der IT Security Officer Informatikdienste führt ein Inventar der bearbeiteten Ausnahmeanträge. Dabei muss nachvollziehbar sein, welche Anträge mit welcher Begründung bewilligt, bzw. abgelehnt wurden, welche Befristungen gelten und welche Auflagen gegebenenfalls mit einer Bewilligung verknüpft sind.

[3] Ausnahmebewilligungen sind befristet, wobei die Bewilligungen bei Ablauf durch den/die Antragsteller/in überprüft und gegebenenfalls ein neues Gesuch gestellt wird.

Artikel 13 Einstellung der Nutzung externer IKT-Services bei andauernder Nichteinhaltung verbindlicher Vorgaben

Bei der Nutzung von externen IKT-Services müssen die gesetzlichen Anforderungen und interne Vorgaben der ETH Zürich eingehalten werden. Der/die Direktor/in der Informatikdienste und der/die Chief Information Security Officer können verfügen, dass ein externer IKT-Service nicht verwendet werden darf, bzw. dessen Verwendung eingestellt werden muss, wenn dieser andauernd rechtliche, vertragliche oder interne Vorgaben der ETH Zürich verletzt.

Schlussbestimmungen

Artikel 14 Verantwortung für die Verordnung

Die Verordnung «IT-Richtlinien und IT-Grundschutz der ETH Zürich» wird durch die Abteilung Informatikdienste erarbeitet, jährlich überprüft und dem Vizepräsidenten für Infrastruktur und dem Chief Information Security Officer der ETH Zürich jährlich vorgelegt.

Artikel 15 Aufhebung bisherigen Rechts

Die folgenden Erlasse werden aufgehoben:

1. Standards für Verantwortlichkeiten und Systempflege vom 6. Februar 2003 (RSETHZ 203.23)

2. Die IT-Best Practice Rules, Version 1.4 vom 6. März 2019

3. Vorherige Versionen der IT-Richtlinien und IT-Grundschutzvorgaben (RSETHZ 203.23)

Artikel 16 Übergangsbestimmung

Ausgabe 2022 der IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich sind bis spätestens März 2023 umzusetzen.

Artikel 17 Inkrafttreten

Diese Richtlinien treten am 1. August 2022 in Kraft.

Zürich, 14.07.2022

Prof. Dr. Ulrich Weidmann
Vizepräsident für Infrastruktur
ETH Zürich

Dr. Domenico Salvati
Chief Information Security Officer
ETH Zürich

Anhang: Passwort- und PIN-Regeln der ETH Zürich

1. Passwörter

a) Passwörter müssen komplex und schwer zu erraten sein. Namen, Geburtsdaten, Telefonnummern, Buchstaben- und Zahlenfolgen, Begriffe aus Wörterbüchern oder ähnliche leicht zu erratene Begriffe, dürfen nicht verwendet werden.

b) Sofern technisch möglich, müssen Passwörter mindestens:
   - 12 Zeichen lang sein[34]
   - Mindestens drei der folgenden Kategorien enthalten
     - Grossbuchstaben
     - Kleinbuchstaben
     - Zahlen
     - Sonderzeichen

c) Bei einem Passwortwechsel muss ein neues, bisher nicht verwendetes Passwort gewählt werden.

d) Das Passwort für das Netzwerk der ETH Zürich (Radius-Authentisierung) muss verschieden von jedem der anderen Passwörter (LDAP, Active Directory etc.) sein.

e) Ein im privaten Umfeld eingesetztes Passwort darf nicht für ein Benutzerkonto an der ETH Zürich eingesetzt werden und umgekehrt.

f) Vom Hersteller voreingestellte Passwörter müssen unmittelbar nach Inbetriebnahme der IT-Systeme geändert werden.

g) Initialpasswörter, die beispielsweise bei der Eröffnung eines neuen Benutzerkontos vergeben werden, müssen bei der ersten Nutzung des Benutzerkontos geändert werden.

h) Bei Missbrauch eines Benutzerkontos oder bei Verdacht auf Missbrauch, muss das betroffene Passwort von einem sicheren IT-System aus unmittelbar gewechselt werden.

i) Ändert sich der Kreis der für den Zugriff auf ein geteiltes Benutzungskonto berechtigten Personen, ist das Passwort zu ändern, sofern dies technisch möglich ist.

[34] Ausnahme: Für das Netzwerk der ETH Zürich (RADIUS-Authentisierung) ist eine Länge von 10 Zeichen ausreichend.

2. PINs

a) Kommen PINs zum Schutz von IT-Systemen zum Einsatz, müssen diese, sofern technisch möglich, mindestens 6-stellig sein.

b) PINs müssen schwer zu erraten sein. Geburtsdaten, Zahlenfolgen (wie 123456) oder Wiederholungen (z.B. 111111) sind nicht erlaubt.

c) Bei Missbrauch oder Verdacht auf Missbrauch, muss die betroffene PIN gewechselt werden.

d) Beim Wechsel einer PIN muss eine neue, bisher nicht verwendete PIN gewählt werden.

e) Vom Hersteller voreingestellte PINs müssen unmittelbar nach Inbetriebnahme der IT-Systeme geändert werden.

f) Ändert sich der Kreis der Personen, die mit einer gemeinsamen PIN arbeiten, ist die PIN zu ändern, sofern dies technisch möglich ist.