Informationssicherheitsrichtlinie zur IT Nutzung

OA1002-03

Group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1002-03
Dokumententitel:	Informationssicherheitsrichtlinie zur IT Nutzung
Fachlich Verantwortlicher:	Andreas Badry
Zuständiger Bereich:	Informationssicherheit
Geltungsbereich:	group24 AG
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Christian Hornhues / Marc Eismann
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung
0.1	09.09.2022	Sandra Kiemes	Initiale Erstellung
0.2	09.09.2022	Andreas Badry	Anpassung auf die group24
0.3	20.10.2022	Andreas Badry	Anpassung auf die group24

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues / Marc Eismann	Ersterstellung und Freigabe
V1.1	15.11.2023	Marc Eismann	Review 2023

1 EINLEITUNG

1.1 Ziel und Zweck

Ziel und Zweck dieses Dokumentes ist es, allen (internen und externen) Mitarbeiter/innen der group24 eine Organisationsanweisung zur Benutzung der DV-/IT-Systemen in die Hand zu geben, damit sie sich bei der Benutzung von DV-/IT-Systemen, insbesondere des Internets, verantwortungsbewusst im Sinne des Unternehmens verhalten können. Angesichts des Risikopotentials sind die folgenden Weisungen für alle Mitarbeiter/innen verbindlich und strikt zu befolgen.

1.2 Hintergrund der Sicherheitsmaßnahmen

Die Unternehmens-IT besonders die Cloud-Services sind eine rasant wachsende und verändernde Umgebung mit allen Vor- und Nachteilen eines offenen weltweiten Netzes. Nützliche wie auch unwichtige Informationen, auch krimineller Natur, sind verfügbar. Die erste Priorität der unternehmensweiten Sicherheit bezogen auf IT Services ist, Mitarbeitern/innen eine Nutzungsmöglichkeit zu bieten bei gleichzeitiger Sicherstellung des Schutzes der Unternehmens-IT und Informationen sowie der Berücksichtigung von Kundenvorgaben und -interessen.

1.3 Gefahrenpotential

Es ist wichtig, sich der Tatsache bewusst zu sein, dass

- die IT auch von Personen benutzt wird, die nicht immer das Wohl des Unternehmens im Auge haben;
- alle ausgetauschten Informationen von einer Vielzahl unbekannter Personen (Kriminelle, Spione, Saboteure, Geheimdienste etc.) gelesen und missbraucht werden können;
- Computer-Viren, Computer-Würmer, Trojanische Pferde oder sonstige Schädlinge unkontrolliert verbreitet und große materielle und immaterielle Schäden verursachen können.

1.4 Sicherheitsmaßnahmen des Unternehmens

Ein Schutz vor den möglichen Gefahrenpotentialen in unserem Unternehmen kann nur dann gewährleistet werden, wenn alle betroffenen Mitarbeiterinnen und Mitarbeiter des Unternehmens mit Zugang zu den IT Services diese Arbeitsanweisung beachten und danach handeln.

1.5 Persönlicher und räumlicher Geltungsbereich

Diese Arbeitsanweisung gilt für alle Mitarbeiterinnen und Mitarbeiter des Unternehmens. Dazu gehören alle beschäftigten Personen (interne und externe), Auszubildende und Aushilfen, mit denen das Unternehmen Verträge zur Leistungserbringung vereinbart hat. Neue Versionen ersetzen die alten Versionen dieses Dokuments vollständig, sofern dies nicht anders ausgewiesen ist.

1.6 Aushändigung

Diese Arbeitsanweisung und Nutzungsvereinbarung wird an alle Mitarbeiter in zweifacher Ausfertigung ausgehändigt, unabhängig davon, ob sie zurzeit bereits eine Zugangsberechtigung zu DV-/IT-Systemen besitzen.

2 SCHUTZBEDARFE UND INFORMATIONS-SICHERHEITSMAßNAHMEN FÜR IT-SYSTEME

Alle IT-Systeme müssen entsprechend ihren Schutzbedarfen geschützt werden. Die Schutzbedarfe ergeben sich aus den unterstützten Geschäftsprozessen und auf Basis der verarbeiteten Daten und der damit verbundenen Risiken. Zu bedenken sind mögliche Schäden, die mit einer Beeinträchtigung der betroffenen Anwendung und damit des unterstützten Geschäftsprozesses oder der verarbeiteten Daten verbunden sind.

Bei der group24 wurden die Schutzbedarfskategorien vom Informationssicherheitsbeauftragter folgendermaßen definiert und mit der Geschäftsführung abgestimmt:

2.1 Schutzbedarfskategorie normal

Ein möglicher Schaden hätte begrenzte, überschaubare Auswirkungen auf die group24:

Gesetze/Vorschriften/Verträge	Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.
Selbstbestimmungsrecht	Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen toleriert.
persönliche Unversehrtheit	Die persönliche Unversehrtheit wird nicht beeinträchtigt.
Aufgabenerfüllung	Die Abläufe bei der group24 werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.
Innen-/Außenwirkung	Es droht kein Ansehensverlust bei Kunden und Geschäftspartnern.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden liegt unter 50.000.- Euro.

2.2 Schutzbedarfskategorie hoch

Ein möglicher Schaden hätte beträchtliche Auswirkungen auf die group24:

Gesetze/Vorschriften/Verträge	Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen schwerwiegende juristische Konsequenzen oder hohe Konventionalstrafen.
Selbstbestimmungsrecht	Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten beträchtliche Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert werden.
persönliche Unversehrtheit	Die persönliche Unversehrtheit wird beeinträchtigt, allerdings nicht mit dauerhaften Folgen.
Aufgabenerfüllung	Die Abläufe bei der group24 AG werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.
Innen-/Außenwirkung	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird erheblich beeinträchtigt.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden liegt zwischen 50.000 und 500.000 Euro.

2.3 Schutzbedarfskategorie sehr hoch

Ein möglicher Schaden hätte katastrophale Auswirkungen:

Gesetze/Vorschriften/Verträge	Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen existenzbedrohende juristische Konsequenzen oder Konventionalstrafen
Selbstbestimmungsrecht	Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten ruinöse Auswirkungen auf die gesellschaftliche oder wirtschaftliche Stellung der davon Betroffenen.
persönliche Unversehrtheit	Die persönliche Unversehrtheit wird sehr stark und mit bleibenden Folgen beeinträchtigt.
Aufgabenerfüllung	Die Abläufe bei der group24 AG werden so stark beeinträchtigt, dass Ausfallzeiten, die über zwei Stunden hinausgehen, nicht toleriert werden können.

Innen-/Außenwirkung	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird grundlegend und nachhaltig beschädigt.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden liegt über 500.000 Euro.

3 ANSCHAFFUNG, ENTWICKLUNG, TEST UND PRODUKTIVER BETRIEB

Diese Richtlinie behandelt Anforderungen an Entwicklungs- Test- und Produktionssysteme, an das Änderungsmanagement und zur Beschaffung und dem Lifecycle.

3.1 Entwicklungs-, Test- und Produktionssysteme

Die folgenden Anforderungen gelten für IT-Systeme, die von der Group24 betreiben werden.

Das erforderliche Maß an Trennung zwischen Produktions-, Test- und Entwicklungssystemen, das Probleme in der Produktion verhindert, muss identifiziert und mit angemessenen Maßnahmen umgesetzt werden.

Regeln für die Überführung von Software aus dem Entwicklungs- in den Produktionsstatus müssen festgelegt sein.

Die folgenden Punkte zum Schutz der Umgebungen sind risikoorientiert umzusetzen:

1. Änderungen von Anwendungsprogrammen und Customizing (Parametrisierung der Anwendung) in der Produktionsumgebung sind organisatorische Verfahren zu implementieren, die einen Schutz gewährleisten.
2. Wenn Produktionsdaten für Tests genutzt werden, muss die Vertraulichkeit der Produktionsdaten im Testsystem ihrem Schutzbedarf entsprechend geschützt werden.

Ein dokumentierter und mit den Informationssicherheitsbeauftragten abgestimmter Notfall-User-Prozess ist zulässig.

3.2 Änderungsmanagement

Um das Risiko einer fehlerhaften Veränderung von in Betrieb befindlichen Systemen zu minimieren müssen die folgenden Regelungen zur Überwachung von Änderungen für produktive IT-Systeme und Anwendungen in Betracht gezogen werden:

1. Änderungen an IT-Systemen dürfen nur nach angemessen ausgiebigen und erfolgreichen Tests eingespielt werden. Bei Tests sind neben der korrekten Funktionalität auch die Benutzbarkeit, Sicherheit, Nebenwirkungen auf andere Systeme sowie Bedienerfreundlichkeit zu bedenken. Sie sollten auf separaten Systemen durchgeführt werden.
2. Eine Rollback-Strategie muss aufgesetzt sein, bevor Änderungen durchgeführt werden.

Jede Entscheidung auf eine neue Version zu aktualisieren, muss die geschäftlichen Anforderungen für die Änderung und die Sicherheit der Version berücksichtigen.
Dies wurde festgehalten im Prozess: Group24_P2009_Change_Management

3.3 Beschaffung und Lifecyle

Eingekaufte Software, die in betriebenen IT-Systemen eingesetzt wird, kann in dem vom Hersteller unterstützten Maß gewartet werden.

Abhängig vom Schutzbedarf ist der Abschluss von Wartungsverträgen zu entscheiden sowie der Support durch den Softwarehersteller sicherzustellen.

4 SCHWACHSTELLENMANAGEMENT / VIRENSCHUTZ

4.1 Schwachstellenmanagement

Die Verantwortlichen eines IT-Systems müssen ihr IT-System regelmäßig oder anlassbezogen aktualisieren, um Schwachstellen zu behandeln.

- Die Verantwortung für das Schwachstellenmanagement trägt der/die Verantwortliche eines IT-Systems. Die operative Umsetzung kann mittels eines Dienstleisters erfolgen.
- Die Verantwortlichen eines IT-Systems müssen geeignete Prozesse und Kommunikationskanäle etablieren, um über Schwachstellen und zur Verfügung stehende Patches informiert zu werden.
- Die Verantwortlichen eines IT-Systems müssen die aktuell eingesetzte Version (Software) bzw. das aktuell eingesetzte Modell (Hardware) dokumentieren.
- Die Verantwortlichen eines IT-Systems müssen Schwachstellen, die nicht sofort behandelt werden können, bewerten und falls sie ein Risiko für die group24 darstellen an den Informationssicherheitsbeauftragten gemeldet werden.

Technische Schwachstellen müssen durch den Einsatz von aktuellen Virenschutzsoftware und Implementierung eines Patchmanagements verhindert werden.

5 IDENTITÄTS- UND BERECHTIGUNGS-MANAGEMENT

Identitäts- und Berechtigungsmanagement hat zum Ziel, den Zugang zu Informationen und informationsverarbeitenden Systemen angemessen zu regulieren.

Die hier synonym gebrauchten Begriffe Rechte und Berechtigungen umfassen sowohl logische Berechtigungen, die zum Beispiel mit Hilfe von IT-Systemen Zugriff auf Informationen gewähren, als auch physische Berechtigungen, die Zutritt zu Gebäuden oder Räumen gewähren.

5.1 Benutzerkonten

Für Benutzerkonten, deren Verwaltung in der Verantwortungshoheit der group24 liegt, gilt:

- Einmal vergebene personalisierte Benutzerkonten dürfen nicht erneut einer anderen Person zugeordnet werden.
- Für alle nicht personalisierten Benutzer, insbesondere für den Einsatz technischer Benutzer im Dialogbetrieb (z.B. mit Hilfe von Benutzeroberflächen), muss die Zuordnung jedes Einsatzes zur handelnden Person zweifelsfrei (z.B. durch Dokumentation) nachvollziehbar sein. Das Passwort für die betreffenden Benutzerkonten muss vor missbräuchlicher Nutzung durch geeignete technisch/organisatorische Maßnahmen geschützt werden.

Betrieblich notwendige Ausnahmen von diesen Regelungen sind von den Informationssicherheitsbeauftragten zu genehmigen.

5.2 Berechtigungskonzepte

Im Rahmen der Berechtigungskonzeption sind Berechtigungen und Anwendergruppen abzuleiten.

Das Berechtigungskonzept muss folgende Angaben enthalten:

- die fachlichen und technischen Anforderungen, aus denen sich Berechtigungen und Anwendergruppen ableiten
- die aus den Anforderungen abgeleiteten Anwendergruppen einschließlich der ihnen zugewiesenen Rollen/Profile oder ggfs. Einzelrechte, insbesondere die anwendungsspezifischen Berechtigungen auf Austausch- und Gruppenlaufwerke oder -verzeichnisse,
- die erlaubte Zuordnung von Rollen/Profilen zu Anwendergruppen,
- die privilegierten Berechtigungen,
- alle im System eingerichteten technischen Nutzer und deren verantwortliche Mitarbeitende,

- eine Beschreibung des Antrags- und Vergabeprozesses zum Einrichten, Ändern, Sperren und Löschen von Berechtigungen,
- die zur regelmäßigen Überwachung der Nutzung von Berechtigungen und Überprüfung der eingerichteten Berechtigungen umgesetzten Prozesse

In den Berechtigungskonzepten kann auf bestehende Dokumente verwiesen werden. Für Anwendungen, die durch einen externen Anbieter bereitgestellt werden, ist das Berechtigungskonzept auf die durch die Group24 genutzten Rollen und Berechtigungen zu beschränken.

5.3 Antrags- und Vergabeprozesse für Berechtigungen

Veränderungen an Berechtigungszuweisungen sind ausschließlich über einen definierten Antrags- und Vergabeprozess für ein System zu genehmigen.

Ausgenommen hiervon sind

- Berechtigungen, die sich unmittelbar aus einer offiziell vergebenen Rolle ergeben, die der Mitarbeitende innehat. Diese Berechtigungen erhält bzw. verliert der Mitarbeitende automatisch mit einem offiziell durch den Personalbereich angestoßenen Vorgang.

Den Antrags- und Vergabeprozess werden im Berechtigungskonzept unter Beachtung der folgenden Regeln festgelegt:

1. Berechtigungen dürfen erst nach vollständiger Genehmigung eines Berechtigungsantrags im System eingerichtet werden.
2. Die Berechtigungsanträge sind von der jeweils umsetzenden Stelle nachvollziehbar dokumentiert abzulegen.
3. Ein Ablaufdatum für Externe ist notwendig.

   Ein Berechtigungsantrag, welcher den Berechtigungsumfang erhöht, muss durch die Führungskraft der Person, für die eine Berechtigung beantragt wird.
4. Für einen Berechtigungsantrag, welcher den Berechtigungsumfang ausschließlich reduziert, also nur Löschungen umfasst, ist eine Genehmigung durch den Benutzer, die Führungskraft oder den Informationssicherheitsbeauftragten ausreichen.

Sieht ein Genehmigungsprozess eine Genehmigung durch die Führungskraft des Berechtigungsempfängers vor, gilt folgendes:

- Für technische oder nicht personalisierte Benutzerkonten genehmigt die Führungskraft der Person, die für das Benutzerkonto verantwortlich ist.

5.4 Privilegierte Berechtigungen

Privilegierte Berechtigungen (synonym: Sonderrechte oder administrative Berechtigungen) umfassen weitergehende Veränderungsmöglichkeiten von IT-Systemen oder Software-Komponenten, als für die fachliche Anwendung des jeweiligen IT-Systems erforderlich ist.

Zu den privilegierten Berechtigungen gehören somit:

1. Berechtigungen zur Installation, Verwaltung, Instandhaltung und Instandsetzung von Anwendungen, Datenbanken, Betriebssystemen oder Infrastrukturkomponenten
2. Berechtigungen zum Einrichten, Ändern, Löschen von Benutzer- oder technischen Konten oder Vergabe von Rechten, soweit diese Rechte nicht ausschließlich den Zugriff auf Daten von zeitlich und inhaltlich abgegrenzten Projekten beinhalten.
3. Berechtigungen zum Verändern von übergreifenden Systemeinstellungen und Konfigurationen, die über persönliche Benutzereinstellungen hinausgehen

Die folgenden Regelungen sind für Produktionssysteme umzusetzen:

1. Es ist eine Minimierung privilegierter Berechtigungen nach dem Least-Privilege-Prinzip anzustreben. Für den täglichen Gebrauch ist daher die Nutzung von Konten mit privilegierten Berechtigungen soweit sinnvoll möglich zu minimieren.
2. Lokale Administrationsrechte auf Client-PCs sowie für Server, auf welchen produktive Anwendungen betrieben werden, sind ausschließlich für besonders gekennzeichnete Konten zulässig. D.h. sind lokale Administrationsrechte notwendig, muss ein separates, personalisiertes Zusatzkonto eingerichtet werden.

Mit diesen Zusatzkonten ist es unzulässig, das E-Mail System oder das Internet zu nutzen. Dies soll soweit möglich durch technische Maßnahmen unterstützt werden.

6 AUTHENTIFIZIERUNGSVERFAHREN

Zugänge auf IT-Systeme werden durch Authentifizierungsverfahren gesteuert. Authentifizierungsverfahren sollen so wenig Informationen wie möglich über das IT-System preisgeben.

Das genutzte Verfahren zur Überprüfung der Anmeldung in einem IT-System sind Passwörter. Bei Endgeräten sind unterstützende Autorisierung Methoden wie PIN, FaceID, Fingerabdruck möglich. Vor der Ausweitung dieser Verfahren und bei der Einführung neuer Verfahren ist die Genehmigung der Informationssicherheitsbeauftragten einzuholen.

6.1 Passwörter

Für ein IT-System, das zur Authentifizierung Passwörter verwendet, gilt:

1. Es muss die Verwendung individueller Benutzerkennungen und Passwörter erfordern.
2. Es muss - soweit umsetzbar - angemessene Vorgaben für die Passwortstärke machen. Indikatoren für starke systemseitige Passwortvorgaben sind beispielsweise:
   - Die geforderte Länge des Passworts beträgt mindestens 8 Zeichen.
   - Erlaubt sind möglichst viele Zeichenvarianten wie Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen wie Leerzeichen, ?!%+…).
   - Das IT-System erlaubt keine Passwörter, die für Wörterbuchangriffe anfällig sind oder die Folgen identischer, numerischer oder alphanumerischer Zeichen (bspw. „aaaa", „1111") oder nebeneinanderliegender Tastaturzeichen („asdfgh", "1234") enthalten.
   - Das IT-System erlaubt keine Passwörter, die ein benutzerspezifisches Wort wie Kennung oder Name enthalten.
   - Das IT-System erlaubt bei einem Passwortwechsel dem Benutzer nicht, eines seiner letzten 10 vorher verwendeten Passwörter zu verwenden.
   - Die Komplexität seines Passwortes wird dem Benutzer durch die Einblendung der geschätzten Passwort-Stärke angezeigt.
3. Es darf Passwörter bei der Eingabe auf dem Bildschirm nicht oder nur auf Benutzeranforderung anzeigen.
4. Es darf Passwörter nicht unverschlüsselt speichern oder übertragen.
5. Es muss den Benutzern die Möglichkeit bieten, eigene Passwörter zu wählen und diese zu ändern sowie eine Rückmeldung bei Eingabefehlern bereitstellen.
6. Das PW das nicht den Firmennamen enthalten.

Für den Zugang in die M365+ gilt wie auch für group24 gilt zusätzlich:

1. Es muss die Benutzer auffordern, ein Initialpasswort bei der ersten Anmeldung zu ändern.
2. Es muss mindestens eine der folgenden Maßnahmen zum Schutz vor Missbrauch von Passwörtern umgesetzt sein:

- Mehrfaktorauthentifizierung – d.h. neben dem Passwort muss mindestens ein weiterer unabhängiger Faktor wie Besitz (z.B. Token) oder Inhärenz (Biometrie) geprüft werden
- Eine zuverlässige Methode zur Erkennung einer Passwort-Kompromittierung, z. B. der Abgleich von am AD angemeldetem Benutzerkonto mit dem im jeweiligen System genutzten Benutzerkonto
- Die systemseitig vorgegebene Passwortlänge liegt bei mindestens 10 Zeichen

3. Es muss, soweit systemseitig unterstützt, eine Begrenzung der Anzahl möglicher Anmeldungsversuche aktiviert werden.

   Die Übermittlung eines Initialpasswortes mittels einer verschlüsselten E-Mail an die Mailadresse des primären AD-Kontos eines Mitarbeitenden ist zulässig.

6.2 Authentifizierung an Betriebssystemen

Authentifizierungsverfahren an Betriebssystemen von Clients, Servern und mobilen Endgeräten sollten:

- die Anzahl erfolgloser Anmeldeversuche begrenzen
- erfolglose und erfolgreiche Anmeldeversuche protokollieren
- inaktive Sitzungen nach einer vorgegebenen Zeitspanne sperren oder beenden

7 KRYPTOGRAPHIE

Die Notwendigkeit des Einsatzes eines kryptografischen Verfahrens wird im Einzelfall durch mehrere Faktoren bestimmt. Grundlage der Festlegung ist

- der Schutzbedarf der verarbeiteten, gespeicherten oder übertragenen Informationen hinsichtlich ihrer Vertraulichkeit (inklusive Schutzbedürftigkeit personenbezogener oder personenbeziehbarer Daten) und Integrität,
- die konkrete Risikosituation der die Informationen bei ihrer Verarbeitung, Speicherung oder Übertragung ausgesetzt sind,
- bestehende gesetzliche oder vertragliche Verpflichtungen.

Es kann daher keine grundsätzliche Festlegung getroffen werden, wann Informationen mittels kryptografischer Verfahren zu schützen sind – vielmehr wird die Entscheidung in jedem Einzelfall auf Basis des Schutzbedarfs und der Risikoeinschätzung getroffen.

7.1 Anforderungen an kryptografische Verfahren

- Der Einsatz von kryptografischen Verfahren ist zu dokumentieren (Detailspezifikation, Sicherheitskonzept) und bedarf vor der Umsetzung und Betriebsübergabe einer Freigabe durch das IT Sicherheitsmanagement der group24.
- Bei der eines kryptografischen Verfahrens sind die jeweiligen Einflussfaktoren zu erheben und zu dokumentieren, die für den Einsatz relevant sind (siehe Abschnitt 7.3 Einflussfaktoren für kryptografische Verfahren).
- Es werden standardisierte kryptografische Verfahren eingesetzt. Proprietäre kryptografische Verfahren werden grundsätzlich nicht eingesetzt.
- Es finden ausschließlich Verfahren Verwendung, die starke Algorithmen einsetzen. Als stark gilt ein Algorithmus, wenn kein technisch realisiertes Verfahren besteht, das dieses Verfahren innerhalb der Zeit, in der die Daten zu schützen sind, brechen kann. Für die Bewertung von starken Algorithmen und Schlüssellängen sind die aktuellen Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik „TR 02102[1]“ maßgeblich.
- Jeder (nicht öffentliche) Schlüssel eines eingesetzten kryptografischen Verfahrens hat den gleichen Schutzbedarf, wie die mit ihm geschützten Informationen. Der Schutz der eingesetzten Schlüssel muss bei der Ausarbeitung des Sicherheitskonzepts zwingend berücksichtigt werden.
- Zur Unterstützung kryptografischer Verfahren werden grundsätzlich nur erprobte Produkte und Technologien eingesetzt, die keine risikobehafteten Schwächen oder Sicherheitslücken aufweisen.
- Vom Betreiber eines kryptografischen Produkts wird ein Höchstmaß an Sensibilität bezüglich der Eigeninformation über Schwachstellen im eingesetzten Produkt erwartet.

Updates zur Beseitigung von Sicherheitslücken in kryptografischen Systemen und Anwendungen sind hoch priorisiert zu behandeln.

- Beim Import, Transport und Export von schutzbedürftigen Informationen auf mobilen Endgeräten, Wechselmedien oder über Kommunikationsverbindungen sind diese mittels kryptografischer Verfahren zu verschlüsseln. Dabei sind die geltenden gesetzlichen Bestimmungen der beteiligten Länder zu berücksichtigen.
- Werden Schlüssel von einer zentralen Stelle aus verteilt, so muss gewährleistet werden, dass die Übergabe an den Empfänger ohne Risiko der Kompromittierung durchgeführt werden kann.
- Besteht Verdacht auf die Kompromittierung eines Schlüssels, so ist dieser zu deaktivieren oder zu sperren und durch einen neuen Schlüssel zu ersetzen. Das eingesetzte System bzw. die Applikation müssen diese Funktionalität unterstützen und ihre Anwendung in den betrieblichen Dokumenten beschreiben.
- Jedes eingesetzte kryptografische Verfahren ist mindestens alle 5 Jahre einer Risikoeinschätzung zu unterziehen.

7.2 Anforderungen an die Schlüsselverwaltung

Kryptografische Schlüssel sind vor Veränderung, Verlust und Zerstörung zu schützen. Alle nicht öffentlichen Schlüssel sind vor unbefugter Kenntnis zu schützen. Für die Schlüsselverwaltung sind StandaGroup24 und sichere Methoden zu verwenden:

- Erzeugen von Schlüsseln ist in sicheren Umgebungen mit geeigneten Schlüsselgeneratoren durchzuführen.
- Bei zentralen Einrichtungen zur Erzeugung von Schlüsseln für besonders gefährdete Einsatzzwecke sind physikalische Zufallszahlengeneratoren zu verwenden.
- Die Schlüssel sind über sichere Kommunikationswege an die entsprechenden Benutzer zu verteilen bzw. zu aktualisieren.
- Die Aktivierung der Schlüssel darf erst nach der Übermittlung an den Benutzer erfolgen.
- Aktivierungs- und Deaktivierungsdaten sind für die Begrenzung des Gültigkeitszeitraums zu definieren.
- Die Schlüssel müssen sicher gespeichert werden und im Falle eine Beschädigung oder des Verlustes wiederherstellbar sein.
- Bei der Kompromittierung von Schlüsseln oder beim Austritt von Mitarbeitern sind diese umgehend zu sperren bzw. zu entziehen und nicht weiter zu verwenden.

Alle Aktivitäten der Schlüsselverwaltung sind zu protokollieren und auszuwerten.

7.3 Einflussfaktoren für kryptografische Verfahren

Im Folgenden werden die Einflussfaktoren dargestellt, welche für die Auswahl und den Einsatz von kryptografischen Verfahren zu beachten sind.

7.3.1 Sicherheitsaspekte

- Welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau gilt es zu erreichen?
- Welche kryptographischen Funktionen sind dafür notwendig (Vertraulichkeits- oder Integritätsschutz)?
- Mit welchen Angreifern wird gerechnet (zeitliche und finanzielle Ressourcen, technische Fähigkeiten)?

7.3.2 Technische Aspekte

- Umfeld Schutz: Welchen Schutz bietet das Umfeld, beispielsweise durch infrastrukturelle Sicherheitsmaßnahmen wie Zutrittskontrolle, organisatorische, personelle und technische Maßnahmen?
- IT-Systemumfeld: Welche Technik wird eingesetzt, welche Betriebssysteme, etc.?
- Datenvolumen: Welches Datenvolumen ist zu schützen?
- Häufigkeit: Wie häufig besteht Verschlüsselungsbedarf?
- Performance: Wie schnell müssen kryptographische Funktionen arbeiten (Offline, Online-Rate)?
- Wiederherstellbarkeit: Auf welche Dauer müssen Schlüssel und verschlüsselte Daten wiederherstellbar sein?

7.3.3 Organisatorische Aspekte

- Benutzerfreundlichkeit: Benötigen die Benutzer für die Bedienung kryptographische Grundkenntnisse? Behindert der Einsatz eines Krypto Produkts die Arbeit?
- Zumutbarkeit: Wie viel Belastung durch zusätzliche Arbeit ist für Benutzer zumutbar (Arbeitszeit, Wartezeit)?
- Zuverlässigkeit: Wie zuverlässig werden die Benutzer mit der Krypto Technik umgehen?
- Schulungsbedarf: Inwieweit müssen die Benutzer geschult werden?
- Personalbedarf: Ist zusätzliches Personal erforderlich, z. B. für Installation, Betrieb, Schlüsselmanagement?
- Verfügbarkeit: Kann durch den Einsatz eines Krypto Produkts die Verfügbarkeit reduziert werden?
- Finanzielle Randbedingungen: Wie viel darf der kryptographische Schutz kosten?
- Investitionsschutz: Sind die geplanten kryptographischen Verfahren bzw. Produkte konform zu bestehenden StandaGroup24? Sind sie interoperabel mit anderen Produkten?
- Gesetzliche Vorgaben: Sind alle gesetzlichen und vertraglichen Vorgaben durch das eingesetzte Krypto Verfahren abgedeckt? (sowohl Minimal- als auch Maximalanforderungen)

8 NETZWERKSICHERHEIT

Der Netzbetrieb muss durch den Bereich IT verantwortet werden. Die Verantwortung für den Rechnerbetrieb und den Netzbetrieb müssen in der group24 organisatorisch nicht getrennt sein.

Der Einsatz neuer Netzwerktechnologien oder komplett neuer Produktplattformen in der group24 ist mit den Informationssicherheitsbeauftragten abzustimmen.

Die IT muss folgende Sicherheitsmaßnahmen mit den Informationssicherheitsbeauftragten abstimmen und umsetzen:

1. Risikoorientierte Sicherung und Überwachung der Netzwerke, um einen Befall mit Schadsoftware zu verhindern, aufzudecken und einzudämmen.
2. Unterteilung in logische Netzdienste und/oder physikalische Netze entsprechend gemeinsamer Sicherheitsstufe oder gemeinsamer Nutzungszwecke zur Kontrolle und Begrenzung des Datenflusses innerhalb des Netzes der group24.
3. Vorgaben zur Verhinderung des Datenabflusses auf Netzwerk-Ebene und Überwachung der Einhaltung der Vorgaben.
4. Sofern externe Netzdienste an interne Netzdienste der group24 gekoppelt und genutzt werden:
   - Zwischengeschaltete Sicherheitsmechanismen (bspw. Firewalltechnologie), die den Datenverkehr über Regeln kontrollieren und protokollieren.
   - Die Regeln müssen:
     - definieren, auf welche Netzdienste zugegriffen werden darf und welche Quellen und Ziele von Verbindungen zulässig sind,
     - alle nicht definierten Zugriffe unterbinden.
5. Die Integrität der Kommunikationsknoten muss sichergestellt sein. Bei erhöhten Anforderungen an die Verfügbarkeit sind entsprechende Redundanzen einzuführen.
6. Telekommunikationsverkabelung und -geräte sind gegen Unterbrechung, Störung, Beschädigung und Manipulation riskoorientiert zu schützen. Der physikalische Zugang ist riskoorientiert einzuschränken.
7. Sicherheitsmechanismen für den Zugang zu Netzen:

   Der externe Zugang zu internen Netzen und Netzdiensten hat ausschließlich über die von der group24 bereitgestellten oder genehmigten Netzdienste und Infrastrukturkomponenten zu erfolgen und muss verschlüsselt werden. Andere Zugänge sind soweit möglich technisch zu unterbinden. Die Authentisierung von Benutzern mit Fernzugriff hat mit Mehrfaktor-Authentifizierung zu erfolgen.

   Ausschließlich autorisierte Benutzer oder Geräte dürfen auf Netze der Group24 zugreifen. Falls bei Geräten der Einsatz von NAC (Network Access Control) mit Zertifikaten möglich ist, muss er berücksichtigt werden.

8. Kontrollen, Protokollierung und Dokumentation:
   - Der Zugang zu internen wie externen Netzen hat kontrolliert zu erfolgen und muss protokolliert werden.
   - Sämtliche Änderungen an Netzen und Netzdiensten sind zu dokumentieren (Betriebshandbuch Netzwerk)
   - Die Protokollierung und Überwachung sicherheitsrelevanter (administrativer) Aktivitäten an den relevanten Netzwerkkomponenten muss aktiviert und sichergestellt sein. Die Protokolle müssen vor einfacher Veränderung geschützt sein.

9 CLIENTS, MOBILE ENDGERÄTE UND SERVER

Für alle Gerätetypen und Server gilt:

1. Alle Geräte und virtuellen Clients und Server müssen anhand eines eindeutigen Indentifikationsmerkmals inventarisiert werden.
2. Abhängig vom Schutzbedarf dürfen nur Betriebssysteme und Software eingesetzt werden, die durch den Hersteller mit Sicherheits-Updates versorgt werden.

Für SmartPhones und Tablets mit iOS oder iPadOS gilt:

1. Alle Geräte müssen über eine Management-Software (Microsoft Intune) zentral verwaltet werden.
2. Alle Geräte müssen mit einer Software ausgestattet sein, die Manipulationen am System (Jailbreak, Rooting etc.) erkennt.
3. Geschäftliche und private Daten und Applikationen müssen technisch voneinander isoliert werden.
4. Ein Abfluss von geschäftlichen Daten über Schnittstellen (Zwischenablage, WLAN, Bluetooth, USB etc.) ist zu unterbinden.
5. Integrierte Cloud-Dienste müssen deaktiviert werden.
6. Die Sprachsteuerung ist zu deaktivieren.
7. Der Speicher muss verschlüsselt sein.
8. Die Kommunikation zwischen Endgerät/Apps und Bankinfrastruktur muss verschlüsselt erfolgen.
9. Der Zugriff auf das Gerät muss geschützt sein (PIN, Face-Unlock etc.).

Für Clients mit Windows 10 gilt:

1. Alle Geräte sind angemessen gegen Diebstahl zu sichern.
2. Der Zugang zum BIOS ist zu sichern (Passwort).
3. Das Betriebssystem ist sicher zu konfigurieren (Herstellerempfehlungen, StandaGroup24 oder Best-Practices etc.).
4. Lokale Laufwerke und Partitionen müssen verschlüsselt werden.
5. Dateien müssen bei Zugriff automatisch durch Virenscanner überprüft werden (On-access scanning).
6. Die Ausführung von aktiven Inhalten (Makros, Skript-Code) in Office- und PDF-Dateien ist einzuschränken.
7. Schnittstellen zur Dateiübertragung (Bluetooth, USB, Infrarot etc.) müssen eingeschränkt werden.

Für Server mit Windows-Server-Betriebssystem, GNU/Linux oder Unix gilt:

1. Für jedes Betriebsystem muss die Serverinstallation und an gängige StandaGroup24, Herstellervorgaben oder Best-Practices angelehnt ist.
2. Das Betriebssystem muss durch einen Virenscanner geschützt werden.

3. Dateien müssen beim Zugriff automatisch durch einen Virenscanner überprüft werden (On-access scanning).
4. Out-of-Band-(OOB-)Fernwartungsschnittstellen der Server-Hardware müssen gesichert werden.
5. Der Internetzugriff via Browser ist auf Servern nicht gestattet, solange dies nicht für administrative Aufgaben notwendig ist, und muss wenn möglich über technische Maßnahmen eingeschränkt werden.

10 DATENSICHERUNG

Bei der Datensicherung sind zu unterscheiden Backups und Archivierung.

Backups sind für das Business Continuity Management erforderlich. Backups werden bei einem Verlust des operativen Datenbestandes zur Datenwiederherstellung genutzt. Die gesicherten Daten müssen gemäß der Verfügbarkeitsanforderungen der Geschäftsprozesse wieder eingespielt werden können.

Die Archivierung ist die langfristige und unveränderbare Aufbewahrung von Daten. Der Zugriff auf diese Daten ist im Rahmen des Produktiv- oder Regelbetriebs nicht erforderlich. Die Aufbewahrung erfolgt normalerweise auf Basis rechtlicher oder regulatorischer Anforderungen.

Abhängig vom Bedarf erstellt die IT ein Datensicherungskonzept. Hinsichtlich Backups ergibt sich der Bedarf aus dem Schutzbedarf des IT-Systems. Hinsichtlich Archivierung ergibt er sich aus rechtlichen Anforderungen.

Das Datensicherungskonzept deckt folgende Punkte ab:

Backups:

1. Die Erstellung von Backups
2. Die Wiederherstellung von Backups (Restore)
3. Der Zugriff auf Backups (einschließlich des physischen Schutzes, wie z.B. der Aufbewahrung getrennt von den Originaldaten)
4. Umfang (z. B. komplette oder differentielle Datensicherung) und Häufigkeit der Backuperstellung
5. Die Überprüfung von Backup-Medien
6. Regelmäßige, mindestens jährliche stichprobenartige Tests der Wiederherstellung in der erforderlichen Wiederherstellungszeit (RTO, Recovery Time Objective)

Archivierung (sofern relevant):

1. Die Erstellung von Archiven
2. Das Lesen von Archiven
3. Der Zugriff auf Archive (einschließlich des physischen Schutzes, wie z.B. der Aufbewahrung getrennt von den Originaldaten)
4. Umfang und Häufigkeit der Archivierung
5. Die Überprüfung von Archiven

11 PROTOKOLLIERUNG, ALARMIERUNG, ÜBERWACHUNG, ZEITSYNCHRONISATION

Um Probleme bei Informationssystemen zu identifizierten und Schäden zu verhindern, müssen risikoorientiert definierte Ereignisse, wie z.B. Fehler oder besonders kritische Administrationstätigkeiten, protokolliert und überwacht werden.

11.1 Protokollierung und Alarmierung

Auditprotokolle (Protokolle, Logs, Logfiles) halten Benutzeraktivitäten, Fehler und Informationssicherheitsvorfälle fest. Sie müssen für einen definierten Zeitraum verwahrt werden für die Überwachung der IT-Systeme. Kritische Benutzeraktivitäten, Fehler und Informationssicherheitsvorfälle (Events) lösen Alarme aus.

Auditprotokolle dürfen private und vertrauliche persönliche Daten enthalten. Angemessene Maßnahmen zur Einhaltung des Datenschutzes müssen getroffen werden.

So weit möglich dürfen System-Administratoren nicht berechtigt sein, Aufzeichnungen ihrer eigenen Aktivitäten zu löschen oder das Aufzeichnen zu deaktivieren.

Protokollierungseinrichtungen und Informationen aus Protokollen müssen risikoorientiert vor Verfälschung und unbefugtem Zugang geschützt werden, insbesondere vor

- Änderungen der protokollierten Nachrichtentypen,
- Modifikation oder unbefugter Löschung von Protokolldateien und
- vor der Überschreitung der Speicherkapazität des Speichermediums, auf dem die Protokolle geführt werden.

11.2 Überwachung

Die Überwachung der IT-Systeme durch die Auswertung und Bearbeitung der Protokolle und/oder durch die Bearbeitung von Alarmen muss risikoorientiert erfolgen.

Wie häufig die Ergebnisse der Überwachungsaktivitäten überprüft werden hängt von den adressierten Risiken ab.

Es gelten folgende Grundsätze:

1. Nicht alle Auditprotokolle müssen überwacht und ausgewertet werden. Im Regelfall dienen sie nur der Aufklärung von Fehlern oder Systemproblemen sowie zu Revisionszwecken (interne und externe Prüfer).
2. Zur Fehlervermeidung kann es risikoorientiert angemessen und notwendig sein, bestimmte Änderungen in Auditprotokollen vollständig oder in Stichproben zu kontrollieren.

3. Es ist i.d.R. nicht notwendig, abgewiesene Zugriffsversuche zu protokollieren und auszuwerten, wenn die Abweisung erfolgreich ist und die Anzahl der Fehlanmeldungen an Systemen begrenzt ist (und damit Brute-Force-Angriffe verhindert werden).
4. Die Verarbeitung inkl. der Auswertung und Nutzung von Auditprotokollen ist eine Verarbeitung personenbezogener Daten. Die Vorschriften des Datenschutzes sind einzuhalten.

Die Reaktion auf protokollierte Events und Alarme liegt in der Verantwortung der für den Betrieb Zuständigen. Es muss klare Regeln für den Umgang mit gemeldeten Fehlern geben, also welche Events weitere Maßnahmen oder Eskalationen erfordern, bspw. einen Incidentprozess.

12 VERBINDLICHKEIT DER REGELUNGEN

12.1 Verbindlichkeit der Regelungen

Die im Anhang aufgeführten, veröffentlichten und in Kraft gesetzten Dokumente gelten als Anlage zu dieser OA und sind für alle Mitarbeiter verbindlich.

Sie sind insoweit Bestandteil dieser Organisationsanweisung.

12.2 Ausnahmeregelung

Sollte eine gültige Regelung für einzelne Systeme oder Prozesse, aus welchen Gründen auch immer, nicht umsetzbar sein, so kann der IT Security Manager für dieses System bzw. diesen Prozess eine Ausnahme von den Regeln genehmigen. Die Entscheidung des IT Security Manager erfolgt risikobasiert.

Diese Ausnahmen sind zentral vom IT Security Manager zu dokumentieren.

13 VERSTÖßE UND SANKTIONEN

Verstöße gegen diese Sicherheitslinie und die darunter liegenden Sicherheitsgrundsätze sind nicht tolerier-bar. Sie können daher zu Disziplinarmaßnahmen, arbeitsrechtlichen Maßnahmen oder gar zu Straf- und/oder zivilrechtlichen Verfahren führen.