|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Groupware - kollaborative Software/Lösungen"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300055 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc82704588)

[Dokumentenhistorie 3](#_Toc82704589)

[Inhaltsverzeichnis 4](#_Toc82704590)

[Allgemeine Festlegungen 5](#_Toc82704591)

[Ziel / Zweck 5](#_Toc82704592)

[Geltungsbereich 5](#_Toc82704593)

[Zuständigkeiten 5](#_Toc82704594)

[Genehmigungs- und Änderungsverfahren 6](#_Toc82704595)

[Aufbau des Dokuments 6](#_Toc82704596)

[Sicherheitsrichtlinie „Groupware - kollaborative Software/Lösungen" 7](#_Toc82704597)

[Basismaßnahmen 7](#_Toc82704598)

[Sichere Installation von Groupware-Systemen (APP.5.1.A1) 7](#_Toc82704599)

[Sichere Konfiguration der Groupware-Clients (APP.5.1.A2) 7](#_Toc82704600)

[Sicherer Betrieb von Groupware-Systemen (APP.5.1.A3) 7](#_Toc82704601)

[Datensicherung Archivierung bei Groupware (APP.5.1.A4) 8](#_Toc82704602)

[Planung des sicheren Einsatzes von Groupware-Systemen (APP.5.1.A7) 8](#_Toc82704603)

[Spam- und Virenschutz auf dem E-Mailserver (APP.5.1A22) 8](#_Toc82704604)

[Standardmaßnahmen 9](#_Toc82704605)

[Festlegung von Vertretungsregelungen bei E-Mail-Nutzung (APP.5.1.A6) 9](#_Toc82704606)

[Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer (APP.5.1.A12) 9](#_Toc82704607)

[Umgang mit SPAM durch Benutzer (APP.5.1.A16) 10](#_Toc82704608)

[Auswahl eines Groupware- oder Mail-Providers (APP.5.1.A17) 10](#_Toc82704609)

[Erweiterter Spamschutz auf dem E-Mailserver (APP.5.1.A18) 10](#_Toc82704610)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc82704611)

[Ende-zu-Ende Verschlüsselung (APP.5.1.A21 - CI) 11](#_Toc82704612)

[Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen (APP.5.1.b.d.A1 - CIA) 11](#_Toc82704613)

# Allgemeine Festlegungen

## Ziel / Zweck

Als Groupware (auch kollaborative Software genannt) werden Anwendungen und Systeme bezeichnet, mit denen mehrere Personen (Gruppen) über räumliche bzw. zeitliche Distanzen hinweg zusammenarbeiten können. Mithilfe von Groupware-Systemen können Gruppen untereinander und miteinander kooperieren und Termine abstimmen. Dokumente und Daten lassen sich durch Groupware von mehreren Benutzern gleichzeitig verwenden und bearbeiten, wodurch der Informationsfluss effizienter gestaltet wird.

Unter dem Begriff Groupware-Systeme werden unter anderem der Groupware-Server, die zugehörigen Groupware-Clients und die erforderlichen Groupware-Dienste zusammengefasst. Neben den Basisfunktionen, wie z. B. Projektmanagement, E-Mail, Kalender oder Notizbuch, bieten neuere Applikationen auch Social-Media-Erweiterungen an, durch die Mitarbeiter noch besser kommunizieren und kooperieren können.

Ziel dieser Sicherheitsrichtlinie ist es, Informationen zu schützen, die in und mit Groupware Lösungen abgelegt, verarbeitet oder übertragen werden. Dazu müssen die für Groupware eingesetzten IT-Komponenten und deren Schnittstellen angemessen abgesichert und geeignete Verfahrensweisen etabliert werden. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines APP.5.1 „Allgemeine Groupware" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Groupware - kollaborative Software/Lösungen“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Groupware - kollaborative Software/Lösungen"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Sichere Installation von Groupware-Systemen (APP.5.1.A1)

Alle benötigten Komponenten für Groupware-Systeme sind entsprechend der geplanten und abgestimmten Systemlandschaft der <Institution> sicher zu installieren und zu konfigurieren. Bei der Nutzung von Cloud-basierten Groupware-Lösungen ist im Rahmen eines Tests (Proof-of-Concept) zu verifizieren, ob eine Konfiguration entsprechend den sicherheitstechnischen und datenschutzrechtlichen Vorgaben möglich ist. Nicht genutzte Komponenten des Groupware-Systems sind zu deaktivieren. Sofern Zugänge zum Groupware-System mittels Passwortes abgesichert werden, sind die internen Vorgaben der <Institution> einzuhalten. Zur Vorbeugung von Manipulationen an den Installationsmedien, sind diese Medien vor unbefugtem Zugriff zu schützen und in Notfallsituation den verantwortlichen Administratoren für die Wiederherstellung zur Verfügung zu stellen.

### Sichere Konfiguration der Groupware-Clients (APP.5.1.A2)

Die Groupware-Clients der Mitarbeitenden sind durch die verantwortlichen Administratoren maximal sicher vor zu konfigurieren. Jegliche sicherheitstechnischen und datenschutzrelevanten Änderungen der Konfiguration durch den Mitarbeitenden sind zu unterbinden. Generell dürfen Passwörter nicht im Klartext gespeichert werden.

Bevor Dateianhänge auf dem Groupware-Client ausgeführt werden, sind die Dateianhänge von einem Malware-Schutzprogramm auf Schadsoftware zu überprüfen. Zur Reduzierung des Angriffsvektors sind Groupware-Clients so zu konfigurieren, dass eventuell vorhandenen HTML-Code in E-Mails nicht automatisch durch den Groupware-Client interpretiert wird. Vorschaufunktionen für Datei-Anhänge sind so zu konfigurieren, dass Groupware-Clients Dateien nicht automatisch interpretieren. Es sind sichere Einstellungen für E-Mails im HTML-Format, die Vorschaufunktionen und die E-Mail-Filterregeln sowie für die automatische Weiterleitung von E-Mails gewählt. Idealerweise wird eine automatische Weiterleitung von E-Mails nach Extern beschränkt.

### Sicherer Betrieb von Groupware-Systemen (APP.5.1.A3)

Die verantwortlichen Administratoren informieren sich proaktiv und regelmäßig über neu bekannt gewordene Schwachstellen der eingesetzten Groupware-Systeme. Anschließend werden alle sicherheitsrelevanten Servicepacks, Updates und Patches für das jeweilige Groupwareprodukt eingespielt.

Die Verantwortlichen für den IT-Betrieb der Groupware-Lösung müssen Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergreifen. Die Kommunikation innerhalb des internen Netzes der Groupware-Systeme muss angemessen geschützt werden. Für die Kommunikation über öffentliche Netze müssen Groupware-Systeme eine sichere Transportverschlüsselung entsprechend den Vorgaben der <Institution> anbieten. Versenden Groupware-Systeme von sich aus Daten, ist ebenfalls eine sichere Transportverschlüsselung entsprechend den Vorgaben der <Institution> nutzen.

Die <Institution> sollte eine Richtlinie erstellen, in der alle in der jeweiligen Groupware erlaubten Protokolle und Dienste erfasst sind. Insbesondere müssen die Verantwortlichen für den IT-Betrieb den E-Mailserver so einstellen, dass er nicht als Spam Relay missbraucht werden kann und Malware erkennt und vorab festgelegte Malware-Kategorien in E-Mails und deren Anhängen nicht an dem Mitarbeitenden ausliefert.

Werden Nachrichten auf einem E-Mailserver gespeichert, müssen die Verantwortlichen für den IT-Betrieb des E-Mailserver eine Größenbeschränkung für das serverseitige Postfach einrichten. Diese Größenbeschränkung ist geeignet festzulegen.

### Datensicherung Archivierung bei Groupware (APP.5.1.A4)

Die Verantwortlichen für den IT-Betrieb müssen sicherstellen, dass die Daten der Groupware-Systeme regelmäßig gesichert werden. Hierzu muss zuvor definiert werden, wie die gesendeten und empfangenen E-Mails der E-Mail-Clients sowie die E-Mails auf den Servern gesichert werden.

Bei der Benennung der maximal tolerierbaren Wiederherstellungszeit ist zu berücksichtigen, wie notwendig der E-Mail-Service für die Kommunikation mit Kunden und den Sales-Prozessen ist. Zusätzlich ist eine dokumentierte Vorgehensweise zu definieren, wie die Archivierung der E-Mails unter Berücksichtigung der maximal tolerierbaren Wiederherstellungszeit erfolgen soll. Die Regelungen zur Archivierung beinhalten grundsätzlich, wie, wann und wo gesendete und empfangene E-Mails archiviert werden. Bei der Archivierung von E-Mails sind ebenfalls zeitliche und organisatorische Sicherheitsaspekte sowie die Aspekte des Datenschutzes zu beachten. Der erforderliche Zeitraum ist regelmäßig zu überprüfen und die Planung zur Archivierung bei Bedarf zu korrigieren. Ergänzend wurde auch überprüft, wie sich die E-Mails wieder zurückspielen lassen.

### Planung des sicheren Einsatzes von Groupware-Systemen (APP.5.1.A7)

Bevor bei der <Institution> Groupware-Systeme eingeführt werden, ist zu entscheiden für Zweck die Groupware-Systeme genutzt und welche Informationen darauf verarbeitet werden sollen. Die <Institution> muss jede benutzte Funktion einer Groupware-Lösung einschließlich deren Sicherheitsaspekte planen. Zudem ist die Entscheidung zu treffen, ob ein eigener Groupware-Server eingesetzt oder ein Provider genutzt wird. Es sollte darauf geachtet werden, dass die genutzten Groupware-Systeme ausreichend dimensioniert sind. Ebenfalls ist festzulegen, wie die Groupware-Clients auf die Server zugreifen sollen.

Im Rahmen der Planungsphase ist festzulegen, welche Daten unter welchen Rahmenbedingungen übermittelt werden dürfen und wie sich dies auf den Schutzbedarf der Daten und des Groupware-Systems auswirkt. Zusätzlich ist zu beschrieben, wie ein ordnungsgemäßer Dateitransfer gewährleistet werden kann. Die private Nutzung der Groupware-Dienste sowie Umgang der Mitarbeitenden mit Webmail sollte geregelt werden.

### Spam- und Virenschutz auf dem E-Mailserver (APP.5.1A22)

Die Verantwortlichen für den Betrieb der E-Mailserver müssen einen E-Mail-Scanner mit einem integrierten Virenschutzprogramm installieren, der eingehende und ausgehende E-Mails, insbesondere deren Anhänge, auf Spam-Merkmale und schädliche Inhalte überprüft und Regeln zur Behandlung von identifizierter Malware anbieten. Zusätzlich ist eine Verfahrensweise für die Überprüfung verschlüsselter Mails und ruhender Mails zu definieren.

Vor dem Einsatz des E-Mail-Scanners wurden alle Mitarbeitenden und der Data Protection Commissioner informiert.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Festlegung von Vertretungsregelungen bei E-Mail-Nutzung (APP.5.1.A6)

Für jeden Mitarbeitenden sollte ein geeigneter Vertreter für die Bearbeitung von E-Mails benannt werden. Diese können auf das Postfach des Vertretenden zugreifen. Sofern E-Mails weitergeleitet werden, sind die vertretenen Mitarbeitenden mindestens darüber zu informieren. Für die Unterstützung der Vertreterregelungsprozesse sind für Autoreply-Funktionen spezielle Regelungen zu etablieren. Beim Einsatz von Autoreply-Funktionen dürfen keine internen Informationen weitergegeben werden.

Bei der Umsetzung der Vertreterregelungen müssen die datenschutzrechtlichen Aspekte berücksichtigt werden.

### Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer (APP.5.1.A12)

Im Rahmen von Schulungsprogrammen sollten die Mitarbeitenden über potenzielles Fehlverhalten in Bezug auf Groupware sensibilisiert werden. Die Mitarbeitenden sollten auch darüber informiert werden, nicht an E-Mail-Kettenbriefen teilzunehmen oder zu viele Mailinglisten zu abonnieren. Darüber hinaus sind die Mitarbeitenden auf die Gefahren hinweisen, die beim Öffnen von unerwarteten E-Mail-Anhängen drohen können. Die Schulungen sollten die Mitarbeitenden auch davor warnen, die HTML-Darstellung bei unerwarteten E-Mails zu aktivieren.

Grundsätzlich sind die verantwortlichen Administratoren der Groupware-Systeme zu schulen. Hierzu sollte ein mit dem Mitarbeitenden abgestimmter Schulungsplan erstellt werden. Die Schulungsthemen sollten alle sicherheits- und datenschutzrelevanten Bereiche der Groupware-Systeme umfassen. Weitere Themenschwerpunkte für die Administratoren sind:

* Überblick über Lösungen für Kommunikationssicherheit (z. B. S/MIME, TLS)
* Protokollierung
* Sichern und Verwalten von Konfigurationsdaten
* Datensicherung
* Incident Handling
* Disaster-Recovery-Maßnahmen

### Umgang mit SPAM durch Benutzer (APP.5.1.A16)

Um zu verhindern, dass Spam die Posteingänge der Mitarbeitenden erreicht ist eine kombinierte mehrschichtige Verteidigung zu etablieren. Dies beinhaltet mindestens die äußeren Filterebene, die auf der Reputation des Absenders basiert und einer inneren Filterschicht, die eine tiefe Analyse der Nachricht durchführt. Zusätzlich sollte eine DNS-basierte Erkennung von Spam-Domainen in die Verteidigungsstrategie integriert werden. Durch das Zusammenwirken der blockierenden Reputationsfilter und der eingesetzten Antispam-Technologien sollen zur Reduzierung des Verwaltungsaufwandes ca. 99 Prozent der eingehenden Spam-E-Mails mit nahezu null Fehlklassifizierungen erkannt und gelöscht werden.

Bei nicht automatisch, sondern manuell durch den Mitarbeitenden erkannten SPAM-Mails, soll durch den Mitarbeitenden nicht auf die E-Mails geantwortet, Links in der E-Mail nicht gefolgt oder Anhänge nicht ausgeführt werden. Der Einsatz von E-Mail-Filterprogrammen ist mit dem Data Protection Commissioner und den Mitarbeitenden abzustimmen. Für Newsgroups und Mailinglisten sollten ebenfalls Regelungen erstellt werden.

### Auswahl eines Groupware- oder Mail-Providers (APP.5.1.A17)

Wird seitens der <Institution> ein Groupware-Provider beauftragt, sollten die funktionalen Aspekte identifiziert und mit dem möglichen Provider abgestimmt werden. Auch sollte sichergestellt werden, dass der Provider alle erforderlichen Sicherheitsmechanismen umsetzt und dass dessen Server sicher betrieben werden. Benötigte interne Anforderungen werden unter Berücksichtigung juristischer Aspekte schriftlich festgehalten. Alle Mitarbeitenden sollten darüber informiert werden, was bei der Nutzung von externen Groupware-Diensten zu beachten ist.

### Erweiterter Spamschutz auf dem E-Mailserver (APP.5.1.A18)

Die E-Mail-Server überprüfen eingehende E-Mails mittels des Sender Policy Framework (SPF) und mit Hilfe von DomainKeys. Die <Institution> sollten selbst DomainKeys und SPF einsetzen, um von ihnen versendete E-Mails zu authentisieren. Die <Institution> sollten Domain-based Message Authentication, Reporting and Conformance (DMARC) nutzen, um festzulegen, wie von ihnen versendete E-Mails durch den empfangenden E-Mail-Server überprüft werden sollen.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Ende-zu-Ende Verschlüsselung (APP.5.1.A21 - CI)

Die <Institution> sollten eine Ende-zu-Ende-Verschlüsselung etablieren. Für die Verschlüsselung dürfen nur intern freigegebene Protokolle und Algorithmen genutzt werden.

### Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen (APP.5.1.b.d.A1 - CIA)

Für den Ausfall von Groupware-Systemen sollte ein Notfallplan erstellt werden. Dieser sollte bereits existierende Notfallpläne der <Institution> mitberücksichtigen. Die primäre Aufgabe des Notfallplans ist das Aufrechtzuerhalten bzw. wieder in Betrieb nehmen der Groupware-Systeme. Es sind ein Wiederanlaufplan zu erstellen, der beschreibt, wie die Systeme nach einem Ausfall wieder geregelt hochzufahren sind.

Notfallübungen zur Systemwiederherstellung sollten regelmäßig durchgeführt werden. Dabei werden alle Aspekte eines Systemausfalls bzw. einer Kompromittierung berücksichtigt.