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

Sicherheitsrichtlinie "WLAN-Betrieb"

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 Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300038 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "WLAN-Betrieb" | [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](#_Toc81124679)

[Dokumentenhistorie 3](#_Toc81124680)

[Inhaltsverzeichnis 4](#_Toc81124681)

[Allgemeine Festlegungen 5](#_Toc81124682)

[Ziel / Zweck 5](#_Toc81124683)

[Geltungsbereich 5](#_Toc81124684)

[Zuständigkeiten 6](#_Toc81124685)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81124686)

[Aufbau des Dokuments 6](#_Toc81124687)

[Sicherheitsrichtlinie „WLAN-Nutzung" 7](#_Toc81124688)

[Basismaßnahmen 7](#_Toc81124689)

[Sensibilisierung und Schulung der WLAN-Benutzer (NET.2.2.A2) 7](#_Toc81124690)

[Absicherung der WLAN-Nutzung in unsicheren Umgebungen (NET.2.2.A3) 7](#_Toc81124691)

[Standardmaßnahmen 7](#_Toc81124692)

[Verhaltensregeln bei WLAN-Sicherheitsvorfällen (NET.2.2.A4) 7](#_Toc81124693)

[Maßnahmen bei erhöhtem Schutzbedarf 8](#_Toc81124694)

# Allgemeine Festlegungen

## Ziel / Zweck

Über Wireless LANs (Wi-Fi / WLAN) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Hersteller-Konsortium „Wi-Fi Alliance“ ein, das basierend auf dem Standard IEEE 802.11 mit „Wi-Fi“ einen Industriestandard geschaffen hat. Dabei bestätigt die „Wi-Fi Alliance“ mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

WiFi-Netze bieten einen Gewinn an Komfort und Mobilität. Jedoch birgt die Nutzung auch zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen, da drahtlos kommuniziert wird. Daher ist es wichtig, dass neben dem IT-Betrieb auch die Benutzer für die möglichen Gefahren sensibilisiert werden, die entstehen können, wenn WiFi-Netze unsachgemäß verwendet werden. So müssen die Benutzer über die erforderlichen Kenntnisse verfügen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Insbesondere müssen sie wissen, was von ihnen in Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen reagieren sollten, wenn sie Wi-Fi-Netze nutzen.

In dieser Sicherheitsrichtlinie soll aufgezeigt werden, wie WiFi-Netze sicher genutzt werden können. Für die Erstellung der Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines NET.2.2 "WLAN-Nutzung" zurückgegriffen. Anforderungen, mit deren Hilfe WLANs sicher betrieben werden können, sind dagegen nicht Gegenstand des vorliegenden Dokumentes. Darüber hinaus geht das Dokument nicht auf allgemeine Aspekte eines Clients ein.

## 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 „WLAN-Nutzung“ 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 „WLAN-Nutzung"

## Basismaßnahmen

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

### Sensibilisierung und Schulung der WLAN-Benutzer (NET.2.2.A2)

Die Benutzer (Mitarbeiter) von WLAN-Komponenten, vornehmlich von WLAN-Clients, müssen sensibilisiert und zu den im Standard "Benutzer" aufgeführten Maßnahmen geschult werden. Den Mitarbeitern muss genau erläutert werden, was die WLAN-spezifischen Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem müssen sie auf die Gefahren hingewiesen werden, wenn diese Sicherheitseinstellungen umgangen oder deaktiviert werden.

Die Schulungsinhalte sollten immer entsprechend der jeweiligen Einsatzszenarien angepasst werden. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen müssen die Mitarbeitenden jedoch auch die relevanten WLAN-Sicherheitsrichtlinien vorgestellt bekommen. Ebenso müssen sie über die Gefahren sensibilisiert werden, wenn fremde WLANs verwendet werden sollen.

### Absicherung der WLAN-Nutzung in unsicheren Umgebungen (NET.2.2.A3)

Jeder Benutzer eines Hotspots muss die Sicherheitsanforderungen der <Institution> kennen und danach entscheiden, ob bzw. unter welchen Bedingungen ihm die Nutzung des Hotspots erlaubt ist. WLANs, die nur sporadisch genutzt werden, sollten durch die Benutzer aus der Historie gelöscht werden. Wenn möglich, sollten separate Benutzerkonten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen verwendet werden.

Es muss sichergestellt sein, dass sich kein Benutzer mit Administratorrechten von seinem Client aus an externen WLANs anmelden kann.

Vertrauliche Informationen dürfen nur übertragen werden, wenn entsprechende Sicherheitsmaßnahmen umgesetzt und sichere Protokolle verwendet werden.

## Standardmaßnahmen

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

### Verhaltensregeln bei WLAN-Sicherheitsvorfällen (NET.2.2.A4)

Bei WLAN-Sicherheitsvorfällen sollten die Mitarbeiter der <Institution> folgendes umsetzen:

* Sichern der Arbeitsergebnisse
* beenden der WLAN-Zugriffe
* deaktivieren der WLAN-Schnittstellen ihres Clients
* Genaue Dokumentation der Fehlermeldungen und Anomalitäten. Ebenso ist zu dokumentieren, was sie getan haben bevor bzw. während der potenzielle Sicherheitsvorfall eingetreten ist.
* Benachrichtigung vom Service Desk.

## 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).

Anforderungen an einen erhöhten Schutzbedarf werden derzeit nicht durch die <Institution> definiert.