Global Rule A.19

Cyber Security für Infineon Mitarbeitende

RegID	A.19	Version	4.0	Language	de
Summary	Diese Richtlinie beschreibt allgemeine Anforderungen und Verpflichtungen der Cyber und Informationssicherheit für Infineon Mitarbeitende. Dies beinhaltet den Umgang mit klassifizierten Informationen, allgemeine Regelungen (z.B. die private Verwendung), technologiespezifische Anforderungen und das Melden von Cyber Sicherheitsvorfällen.				
Scope	Infineon worldwide				
Intranet homepage of this Rule	**Always check the intranet homepage of this rule for updates.** The homepage provides the full context of this rule in the latest state. You will find references to the most recent versions of • this rule document • supporting documents that may be enforced through this rule • hints and links to other regulations or resources that are relevant in the context of this rule				

Inhaltsverzeichnis

Geltungsbereich 2

I. Umgang mit Informationen & Sicherheitsbestimmungen 2

A. Generelle Sicherheitsbestimmungen 2

B. Umgang mit klassifizierten Informationen 3

1. Umgang 3

a. Intern (restricted) 3

b. Vertraulich & Streng vertraulich 3

2. Übermittlung 3

a. Interne (restricted) 3

b. Vertraulich 3

c. Streng vertraulich 4

3. Speicherung 4

a. Intern (restricted) 4

b. Vertraulich 4

c. Streng vertraulich 4

C. Technologiespezifische Beschränkungen 5

1. E-Mail 5

2. Mobile-/Smartphone 5

3. Datenspeicherung, Backup und Archivierung 5

D. Melden von Cyber-Sicherheitsereignissen und Vorfällen 5

E. Unterstützung von Untersuchungen und Reaktion auf Vorfälle 6

Nachweise 6

Anhang 6

I. Liste der Referenzen 6

Geltungsbereich

Diese Richtlinie wurde in Übereinstimmung mit der Globalen Richtlinie A.1 „Erstellung und Verwaltung von Regelungen“ erstellt.

Sie gilt für alle Mitarbeitende und Mitglieder der Organe aller Infineon Gesellschaften weltweit.

Richtlinieninhalt

Die vorliegende Richtlinie legt Anforderungen für die zulässige und nicht zulässige Nutzung von Infineons Informationssystemen fest. Dies beinhaltet unter anderem Computersysteme, E-Mail-Systeme, Anrufbeantworter, Telefonsysteme, Online-Dienste, Mobiltelefone, Drucker und Scanner. Darüber hinaus werden die Anforderungen an die Mitarbeitenden hinsichtlich des Umgangs mit elektronischen Daten detailliert beschrieben. Zusätzliche Anforderungen für den Umgang mit physischen Informationen (z.B. Ausdrucke von Dokumenten) sind in der Richtlinie A.36 Corporate Security definiert.

I. Umgang mit Informationen & Sicherheitsbestimmungen

A. Generelle Sicherheitsbestimmungen

Alle Cyber- und Informationssicherheitsanforderungen sind auch außerhalb des Büros gültig, etwa bei der Telearbeit oder auf Geschäftsreisen.

Jede Person mit Zugriffsrechten, d. h. mit einem Account, welcher Zugriff auf die Infineons Informationssysteme gewährt, muss in regelmäßigen Abständen am Informationssicherheitstraining teilnehmen.

Die Benutzer*innen müssen sicherstellen, dass alle Geräte (Notebooks, Workstations und Diensthandys) vor unbefugten Zugriff geschützt sind sobald sie unbeaufsichtigt sind,

Jegliche Art von Scannen oder Stören des normalen Datenflusses der Netzwerkkommunikation (unabhängig ob aktive oder passive Form der Aufzeichnung, des Sniffens, der Umleitung oder Cache Poisoning), welche nicht Teil der täglichen Arbeit sind, ist ohne Freigabe des Leiters der Infineon Cyber Security oder eines Vertretenden verboten.

Das Herunterladen jedweder unternehmensbezogener Daten oder Programme auf private Geräte ist untersagt. Die gelegentliche private Nutzung von Workstations, Laptops oder Smartphones darf keine Gefährdung von Werten (Assets) und Netzwerken Infineons zur Folge haben.

Dabei ist besonders Folgendes zu beachten:

- Der Internetzugriff ist grundsätzlich gestattet. Infineon ist nicht verpflichtet vollen Zugriff auf das Internet zu gewährleisten. Es ist untersagt das Internet für unangemessene bzw. illegale Zwecke, wie der Besuch von Internetseiten, welche diskiminierenden, belästigenden, sexuell eindeutigen, gewalttätigen oder auf anderer Weise inakzeptablen Inhalt zeigen, zu nutzen.

- Die Nutzung von E-Mail-Diensten von Dritt-Anbietern ist für die private Nutzung erlaubt. Das Herunterladen oder Öffnen von privat empfangenen Anhängen untersagt.
- Installation von Software: Software oder Apps dürfen nur direkt von der entsprechenden Hersteller-/Entwickler-Website oder über offizielle App-Stores heruntergeladen werden.
- Das Herunterladen von Dateien, welche gegen geltendes Recht verstoßen, ist verboten.

Während der Nutzung von Workstations und Laptops ist das Speichern von privaten Dateien ausschließlich im Ordner "*C:\Users\Your Account Name\No Backup*" erlaubt.

B. Umgang mit klassifizierten Informationen

Die Einstufung der Vertraulichkeit von Daten muss gemäß der Richtline A.47 „Protection Classes for Information Assets“ erfolgen. Die Vertraulichkeitsklassen sind „öffentlich“, „intern (restricted)“, „vertraulich“ und „streng vertraulich“. Sind Informationen nicht klassifiziert, gilt die Standardeinstufung „intern (restricted)“.

Klassifizierte Informationen müssen vor Verlust, Schaden, unerwünschter Veröffentlichung, Manipulation oder Missbrauch jeder Art geschützt werden. Informationen dürfen nicht an Unbefugte und nur an Personen gemäß dem „Need to know“-Prinzip weitergegeben werden.

Zu diesem Zweck müssen klassifizierte Informationen entsprechend den Anforderungen ihrer Vertraulichkeitsklasse, wie unten beschrieben, gehandhabt, übermittelt und gespeichert werden. Für Daten, welche als „öffentlich“ eingestuft wurden, liegen keine gesonderten Anforderungen oder Beschränkungen vor.

1. Umgang

a. Intern (restricted)

Informationen dürfen mit Infineon Mitarbeitenden geteilt werden. Eine Geheimhaltungsvereinbarung (NDA) ist notwendig wenn Unternehmensinformationen mit Externen geteilt werden. Die Informationseigentümer*innen können situationsabhängig entscheiden, dass ein NDA nicht notwendig ist.

b. Vertraulich & Streng vertraulich

Unauthorisierten Personen (Kolleg*innen eingeschlossen) ist es nicht erlaubt bzw. dürfen nicht in der Lage sein Zugriff auf diese Informationen zu erhalten. Die Weitergabe an Externe muss mit einem gültigen NDA abgesichert werden.

2. Übermittlung

a. Interne (restricted)

Interne (restricted) Informationen dürfen nicht über Chat-Services oder Applikationen verschickt werden, welche nicht von Infineon zur Verfügung gestellt oder zuvor freigegeben wurden.

b. Vertraulich

Wenn vertrauliche Informationen geteilt werden, sollten Infineons interne Sprach- & Videosysteme verwendet werden. Das Übermitteln von vertraulichen Informationen über ein öffentlichen Telefonnetz sollte wenn möglich vermieden werden.

Es dürfen ausschließlich authentifizierte und berechtigte Personen an Telefon- bzw. Videokonferenzen, in welchen vertrauliche Informationen geteilt werden, teilnehmen.

Vertrauliche Informationen dürfen nicht über Chat-Services oder Apps, welche nicht von Infineon bereitgestellt oder freigegeben wurden, übermittelt werden.

c. Streng vertraulich

Werden streng vertrauliche Informationen während einer Telefon- oder Videokonferenz geteilt, muss die Verbindung, welche für die Kommunikation genutzt wird, Ende-zu-Ende verschlüsselt und der Service selbst von der Abteilung Cyber Security freigegeben worden sein. Detaillierte Informationen können den Cyber Security Intranetseiten entnommen werden.

Es wird empfohlen die Infineon internen Sprach- & Videosysteme für das Teilen oder Diskutieren von streng vertraulichen Informationen zur Vermeidung unzulässiger Aufzeichnungen zu verwenden. Werden Gespräche, die streng vertrauliche Informationen übertragen, aufgezeichnet, müssen diese Aufzeichnungen verschlüsselt werden.

Streng vertrauliche Informationen dürfen nicht über das öffentliche Telefonnetz geteilt werden.

Es dürfen ausschließlich authentifizierte und berechtigte Personen an Telefon- bzw. Videokonferenzen, in denen streng vertrauliche Informationen geteilt werden, teilnehmen

Streng vertrauliche Informationen dürfen nicht über Chat-Services oder Apps, welche nicht von Infineon bereitgestellt oder freigegeben wurden, übermittelt werden.

3. Speicherung

Das Speichersystem muss für die Speicherung von Daten abhängig der Klassifizierung zugelassen sein.

a. Intern (restricted)

Interne (restricted) Informationen müssen auf von Infineon bereitgestellten oder freigegebenen Systemen gespeichert werden.

b. Vertraulich

Ausschließlich von Infineon bereitgestellte oder erlaubte Speicherorte dürfen zur Speicherung von vertraulichen Informationen verwendet werden.

Bei der Verwendung von Wechseldatenträgern müssen die vertraulichen Daten auf den Wechseldatenträgern mit von Infineon bereitgestellten Verschlüsselungswerkzeugen verschlüsselt werden (Security Tools)***.***

c. Streng vertraulich

Bei der Verwendung von Wechseldatenträgern müssen die streng vertraulichen Daten auf den Wechseldatenträgern mit von Infineon bereitgestellten Verschlüsselungswerkzeugen verschlüsselt werden.

Dedizierte Systeme und Applikationen müssen zur Speicherung von streng vertraulichen Informationen verwendet werden. Müssen Daten auf einem Infineon Standard Client gespeichert werden, muss diese Information separat verschlüsselt werden (Intranet).

C. Technologiespezifische Beschränkungen

1. E-Mail

Generell sind Infineons E-Mail Services nur für geschäftliche Zwecke einzusetzen.

Das Einrichten von automatischen E-Mail-Regeln zur Weiterleitung von E-Mails an externe E-Mail-Adressen ist verboten.

Es dürfen keine externen E-Mail Adressen auf interne Verteilerlisten gesetzt werden.

2. Mobile-/Smartphone

Apps müssen über einen offiziellen App-Store (Infineon App Store, Apple App Store, oder Google Play Store) installiert werden. Ist eine App im Infineon App-Store erhältlich, muss diese auch hierüber bezogen werden.

Es dürfen keine Datenkanäle zu Dritten aufgebaut werden.

Das Synchronisieren von Unternehmensdaten mit Cloud-Services, welche nicht von Infineon bereitgestellt oder freigegeben wurden, ist nicht zulässig. Entsprechende Services dürfen nicht verwendet und müssen deaktiviert werden.

3. Datenspeicherung, Backup und Archivierung

Die private Datenspeicherung sowie die Erstellung von Backups und Archivierung von Infineon Daten sind verboten.

Eigentümer*innen von Informationssystemen sind für die Erstellung von Backups für alle Equipments und Informationssysteme verantwortlich, sofern diese nicht durch die IT betrieben werden. Dies beinhaltet u.a. Labor- oder Produktionscomputer, Smartphones und virtuelle Desktop PCs. Backups müssen nach der Klassifizierung des zugrunde liegenden Systems geschützt werden.

D. Melden von Cyber-Sicherheitsereignissen und Vorfällen

Alle Infineon Mitarbeitenden müssen jedes vermutete oder bestätigte Cybersicherheitsereignis sofort nach Bekanntwerden an das Cyber Defense Center melden. Dies gilt ebenfalls für Meldungen, die von Drittanbietern oder anderen Geschäftspartnern eingehen. Die Mitarbeitenden müssen die folgenden Cyber-Sicherheitsereignisse melden:

- Informationen wurden von nicht authentifiziertem Personal oder Drittanbietern genutzt
- Informationen wurden von Infineons Computersystemen oder Equipment unsachgemäß oder unberechtigt heruntergeladen oder kopiert

- Equipment oder Geräte, welche Daten von Infineon enthalten, sind verloren gegangen oder gestohlen worden
- Equipment oder Geräte, welche Daten von Infineon enthalten, wurden Gegenstand unautorisierter Aktivitäten (z.B. Hacking und Malware)
- Equipment oder Geräte waren im Besitz von Dritten, wie Strafvollzugsbehörden, Einwanderungsbehörden oder Grenzschutzbehörden
- Dritte haben eine potenzielle Sicherheitslücke in Infineons IT-Systemen oder Produkten gemeldet
- Persönliche Daten wurden öffentlich zugänglich gemacht
- Aktives Umgehen von implementierten Sicherheitsmaßnahmen
- Daten von Infineon, welche als intern (restricted) oder höher eingestuft wurden, sind auf einem öffentlich zugänglichen System abrufbar
- Ein externer Dritter fragt nach Geld oder bedroht den Mitarbeitenden (z.B. Cyber-Betrug, Erpressung)

Auch wenn interne oder externe Mitarbeitende nicht sicher sind, ob es sich bei einem vermeintlichen Cyber-Sicherheitsvorfall um einen tatsächlichen Cyber-Sicherheitsvorfall handelt, müssen sie diesen wie hier vorgesehen melden.

E. Unterstützung von Untersuchungen und Reaktion auf Vorfälle

Interne und externe Mitarbeitende müssen bei der Untersuchung von Vorfällen kooperieren. Sie dürfen dabei andere nicht stören, behindern, Vergeltungsmaßnahmen ergreifen oder sie davon abhalten, einen Vorfall zu melden oder bei einer Untersuchung zu kooperieren.

Nachweise

Die Abteilung Cyber Security überwacht sowohl die Teilnahme am Informationssicherheitstraining als auch die Anzahl an gemeldeten Cyber-Vorfällen der Mitarbeitenden.

Alle Dokumente werden entsprechend ihrer Klassifizierung eingestuft.

Anhang

I. Liste der Referenzen

Die folgende Liste enthält alle in diesem Dokument aufgeführten Links.

- Cyber Security
- Cyber Defense Center
- Cyber Security Intranetseiten
- Rule A.36 “Corporate Security”
- Rule A.47 “Protection Classes for Information Assets”

Global Rule A.19, Version 4.0, de

Cyber Security für Infineon Mitarbeitende

Validity

	Date
Publication Date	2021-04-12
Main version valid from	2016-11-28
Expires on	2022-09-30

Change history

Version	Short description of change	Date
4.0	Major Change; Anforderungen wurden zu anderen Regeln verschoben (A.33, A.47, X.22) und der Inhalt überarbeitet.	2021-04-12
3.0	New chapter 'Mobile/Smartphones' added; Last chapter 'Reporting of Security incidents' extended; In other chapters minor (wording) adaptions; Appendix: list of references added	2019-08-12
2.0	Revalidation without changes in content	2018-06-04
2.0	Neue Klassifizierung 'Restricted' ersetzt 'for internal use only'	2016-11-25
1.0	Übersetzung	2015-11-24

Release

	Name	Date
Author	Lang Tobias (IFAG BC CYBER)	2021-04-12
Rules Owner (1st Appr.)	Otto Raphael (IFAG BC CYBER)	2021-04-12
Approver	Schneider Sven (IFAG CFO)	2021-03-31