Global Rule A.19

Cyber Security for Infineon Employees

RegID	A.19	Version	4.1	Language	en
Summary	This Rule describes general obligations and requirements of cyber and information security for employees at Infineon. It covers handling of classified information, general provision (e.g. private use), technology specific requirements and cyber incident reporting.				
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				

Table of content

Scope

This Rule has been released pursuant to the Global Rule A.1 “Creation and management of Regulations”.

It applies to all employees and members of the representative bodies of all Infineon companies worldwide.

Rule content

This Rule establishes requirements for the acceptable and not-acceptable use of Infineon Information Systems, including but not limited to, all computer systems, e-mail systems, voice mail systems, telephone systems, online services, mobile phones, printers and scanners. Furthermore, it details the requirements for employees regarding electronic data handling. Additional requirements for the handling of physical information (e.g. printed documents) are defined in Global Rule A.36 “Corporate Security”.

I. Handling of Information & Security Provisions

A. General Security Provisions

All cyber and information security requirements also apply outside the office such as for teleworking or on a business trip.

Every person with access, i.e. having an account, which grants access to Infineon information systems must regularly participate in the information security training.

Users must make sure that all devices (Notebooks, Workstations and Company Smartphones) are protected against unauthorized access once the devices are unattended.

Any form of scanning or interference with the normal flow of network communications, whether active or passive in the form of recording, sniffing, redirection, or cache poisoning, that is not part of daily business operations, is prohibited without prior approval of the Head of Infineon Cyber Security or a delegated function.

Downloading any business related data or programmes to private devices is prohibited. The occasional private use of workstations, laptops and smartphones must not endanger Infineon assets or networks.

In particular, the following has to be observed:

- Accessing the Internet is permitted. Infineon is not obliged to provide full access to the Internet. Nevertheless, it is prohibited to access the Internet for inappropriate or illegal purposes, including accessing websites that contain discriminatory, harassing, sexually explicit, violent or otherwise inappropriate or illegal content.
- Use of third party email system for private use is permitted. However, downloading or opening privately received attachments is prohibited.
- Installation of software: Software or Apps should only be downloaded directly from the corresponding manufacturer’s or developer’s websites or official app stores.
- Downloading files that violate any laws is prohibited.

While using workstations or laptops it must also be observed, that the storage/backup of private files is solely permitted in the folder "*C:\Users\Your Account Name\No Backup*".

B. Handling of Classified Information

Data confidentiality has to be classified according to Rule A.47 "Protection Classes for Information Assets". Confidentiality protection classes consist of public, restricted, confidential, and strictly confidential. If information is not marked with a classification level, the default classification is "restricted".

Classified information must be protected against loss, damage, unwanted disclosure, manipulation or misuse of any kind. Information must not be disclosed to unauthorized parties and only to people with 'need to know'.

For this purpose, classified information must be handled, transferred or stored according to the requirements of its protection class as outlined below. There are no requirements or specific provisions defined for data classified as "public".

The Cyber Flyer gives guidance and examples for the obligations defined within this Rule.

1. Handling

a. Restricted

Information can be shared with Infineon employees. A non-disclosure agreement (NDA) is required if any company information is shared with an external party. The information owner may decide that a NDA is not necessary on a case-by-case basis.

b. Confidential & Strictly Confidential

Unauthorized persons (this can include colleagues) must not be allowed or able to access that information. Sharing with external parties must be secured with a valid NDA.

2. Transmission

a. Restricted

Restricted information should not be shared over chat-services or applications not provided or approved by Infineon.

b. Confidential

If confidential information is shared, Infineon internal voice & video systems should be used. If possible, confidential information sharing should be avoided via public phone network.

Only authenticated and authorized users must participate in telephone or video conferences with confidential data.

Confidential information must not be shared over chat-services or apps not provided or approved by Infineon. The transmission of confidential data must be end-to-end encrypted.

c. Strictly Confidential

If strictly confidential information is shared or discussed during telephone or video calls, the connection used for communication must be end-to-end encrypted and the service must be

approved by the Cyber Securitydepartment. Detailed information can be found on the Cyber Security intranet pages. It is recommended to use Infineon internal voice & video systems for sharing or discussing strictly confidential information to avoid unapproved recordings. If calls transmitting strictly confidential information are recorded, these recordings must be encrypted.

Strictly confidential information must not be shared via public phone network.

Only authenticated and authorized users must participate in telephone or video conferences with strictly confidential data.

Strictly confidential information must not be shared over chat-services or applications not provided or approved by Infineon.

3. Storage

The storage system must be approved for the storage of data in respect to its classification.

a. Restricted

Restricted information should be stored on Infineon provided or approved systems.

b. Confidential

Only Infineon provided and allowed storage must be used for storing confidential information.

If using removable media, Infineon confidential data on removable media must be encrypted, using encryption tools provided by Infineon (Security Tools).

c. Strictly Confidential

If using removable media, Infineon strictly confidential data on removable media must be encrypted, using encryption mechanisms and technology provided by Infineon.

Dedicated systems and applications must be used for storing strictly confidential information. If data has to be stored on an Infineon Standard Client that information has to be encrypted separately (Intranet).

C. Technology Specific Provisions

1. Email

In general, Infineon's email services must be solely used for business purposes.

Setting up automated email rules to forward emails to external email addresses is prohibited.

Including external email addresses in internal distribution lists is prohibited.

2. Mobile-/Smartphones

Apps must be installed from an official app store (Infineon App Store, Apple App Store, or, Google Play Store). If an app is available in the Infineon App Store, the app must be installed from the Infineon App store.

Data channels to third parties must not be established.

Synchronization of company data with cloud services not provided or approved by Infineon, must not be used and turned off.

3. Data Storage, Backup and Archiving

Private data storage, backups and archives of Infineon data is prohibited.

Information System Owners are responsible for the backup of all non-IT managed equipment and information systems. This includes for example laboratory or production computers, smartphones and virtualized desktop PCs. Backups must be protected according to the classification of the system which is the source for the backup.

D. Report cyber-security events and incidents

All Infineon personnel must report any suspected or confirmed cyber security event to the Cyber Defense Center immediately upon discovery. This includes notification received from any third-party service providers or other business partners. Personnel must report the following cyber-security events:

- Information was used by unauthorized personnel or third parties;
- Information has been downloaded or copied inappropriately from Infineon's computer systems or equipment;
- Equipment or devices containing Infineon data or information have been lost or stolen;
- Equipment or devices containing information have been subject to unauthorized activity (e.g., hacking, and malware).
- Equipment or devices have been in possession by third parties such as law enforcement, immigration officers or border patrol.
- Third parties reported a potential vulnerability in Infineon IT systems or products.
- Personal Data that has been publicly exposed.
- Actively bypassing implemented security measures
- Infineon data classified as restricted or above is accessible on a publicly available system
- An external third party asks for money or threatens you (e.g. cyber fraud, blackmailing).

Even if internal or external personnel are not sure whether a cyber-security event is an actual cyber-security incident they are encouraged to report it as provided herein.

E. Support incident investigations and response

Internal and external personnel must cooperate with incident investigations, and may not interfere, obstruct, prevent, retaliate against, or dissuade others from reporting an incident or cooperating with an investigation.

Proof of evidence

Cyber Security department monitors the participation in the information security training as well as the number of reported cyber incidents by employees.

All documents are labeled according to their classification.

Appendix

I. List of references

The following list shows all links contained in this document

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

Global Rule A.19, Version 4.1, en

Cyber Security for Infineon Employees

Validity

	Date
Publication Date	2022-10-13
Main version valid from	2016-11-28
Expires on	2024-04-30

Change history

Version	Short description of change	Date
4.1	Minor Changes: Formatting, Link addition	2022-10-09
4.0	Major change: Requirements shifted to other Rules (A.33, A.47, X.22) and content updated.	2021-03-22
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	2018-05-07
2.0	Revalidation without changes in content	2017-08-29
2.0	new information classification	2016-11-17
1.0	Initial upload	2015-11-24

Release

	Name	Date
Author	Abreu Charles (IFSSC BC CYBER GRC)	2022-10-09
Rules Owner (1st Appr.)	Otto Raphael (IFAG BC CYBER)	2022-10-13
Approver	Schneider Sven (IFAG CFO)	2021-03-31