Information Security Handbook

Binding for all units of TecAlliance

Ruf, Martin

TecAlliance GmbH
Steinheilstrasse 10
D-85737 Ismaning
Germany

Change history

Source version	Target version	Date	Name	Comment
---	0.0.1	2020-02-10	MRUF	Initial Draft
0.0.1	0.0.2	2020-06-18	MRUF	Alignment within CCS-IT
0.0.2	0.0.3	2020-07-29	MRUF	Removed SW Development Topics, Changed Incident Handling to include CSIRT team
0.0.3	0.0.4	2020-09-03	MRUF	Alignment with the workers' council in Cologne
0.0.4	1.0	2020-10-01	MRUF	Document aligned with CCS-IT, P&O, Finance, BU Heads and workers' council
1.0	1.1	2020-11-02	MRUF	Changed "Clean Desk" to "Clear Desk" to avoid confusion, changes in 5.9 Disposal.
1.1	1.2	2022-11-29	HF, MRUF	Deleted chapter 3.2 ("Information Inventory") Changed in chapter 3.3 (now 3.2): Obligation to information labelling to recommendation; Clearance of public information can now be performed by information owner Added to chapter 6.4 "…the regular check of the last login date of external accounts…" Merged three parts depending on target audience into one Re-Integrated Roles & Definitions, Risk Measurement Method added, fixed formatting, some wording revisions
1.2	1.3	2023-02-01	MRUF	Added 6.4.1 Central Reporting of systems handling user accounts/passwords and 6.7 Mandatory penetration test before go-live

Distribution list

This document should be distributed to every employee of TecAlliance and all its subcompanies.

Responsible for this guideline

Information Security & Privacy

Contact / Author

Martin Ruf

Martin.Ruf@TecAlliance.net

Table of Contents

1 About this document

This document includes all policies for TecAlliance related to Information Security. Nonetheless, it is meant to be helpful and to give you information and guidance when designing, using or modifying our IT systems.

The document's structure is designed to support two use-cases:

1. Giving an overview of relevant topics and guidelines for information security

   If you read this document from beginning to end, you get a pretty good understanding of how information security works at TecAlliance.

2. Helping you in a specific situation you are facing

   If you want to take into account all factors relevant for information security in your specific situation, you should be able to get fast answers by skipping over the headlines and the beginning of each chapter. By reading relevant chapters in detail, you get more guidance and background information.

1.1 How to read it

Every chapter starts with a short statement of its applicability. If the statement is not applicable to the situation you are facing, you can safely skip the chapter.

Every chapter also starts with a paragraph that explains the purpose of the chapter's guidelines. If you are sure you already reach that goal you can also safely skip the chapter.

If the chapter is applicable and you do not reach the goal by other means, consider the guidelines binding.

In case you cannot comply, TecAlliance Risk Management procedures apply. Please refer to the Risk Management chapter to threat the risk resulting from the specific non-compliance.

➲ Note
Notes are not binding. In case of any question, always feel free to contact Information Security & Privacy (security@tecalliance.net)

1.1 Roles & Definitions

1.1.1 IT

The term IT includes every electronical data processing (processes, functionality), information processing and the hard-/software used for that at every part of the organization.

1.1.2 System

The term System describes any combination of physical systems (such as a notebooks), virtual systems(such as a VMs) or applications (such as a web application or a technical service). The term System both includes systems that are in use for company internal purposes (build by TecAlliance or bought/licensed from 3rd party) and systems that we build or provide (e.g. our solutions). A system can be:

- A TecAlliance Solution
- An application we use internally
- A piece of hardware (e.g. IT Equipment)
- A software tool (developed internally or licensed externally)
- A technical service that we consumeor provide

1.1.3 IT Equipment

The term IT equipment references any hardware that is used by TecAlliance. It explicitly also includes media (such as USB pen drives).

1.1.4 System Owner

The System Owner is the individual that is overall responsible for a system. Every system has exactly one owner and every system owner is an employee of the TecAlliance Group. While the System Owner is responsible for every aspect of the system, there may be multiple other System Owners involved, whos' systems are used as components. In this case, they can cover responsibility for parts, but the overall responsibility remains. The system owner is at least responsible for the system design, lifecycle and the way the system is used.

The system owner is determined in this order as the first person being an employee of TecAlliance:

- The individual that built the system
- The individual that ordered the system
- The technical lead of a team that develops the system
- The Product Owner of the Product that contains the system
- The BU Lead in who's responsibility the system runs
- The EVP in who's responsibility the system runs
- The CEO of TecAlliance

System ownership can be delegated within the TecAlliance Group, delegation has to happen explicitly.

Typical examples of System Owners:

- A Product Owner
- A Service Owner
- An Application Owner

2 Security Responsibility

> ➲ Note
>
> At TecAlliance, we value ownership. Ownership includes responsibility for every aspect of the item owned. In case of IT systems, services, solutions and the like, decisions on how a specific functionality is implemented or which configuration settings are appropriate can have a significant security impact. The balance of security and other requirements is part of ownership.

Every individual responsible for a piece of hard-/software, service or solution ("System Owner" as described above) is also responsible for every security aspect of it.

The role of Corporate Information Security is:

- **We are here to help**
  We provide consulting and training. Whenever there is a security-related question, feel free to contact security@tecalliance.net.
- **We create transparency**
  We identify and communicate risks by performing random probes. We inform responsible individuals and escalate where necessary.
- **We drive global topics**
  There are Information Security topics where a global solution makes sense. We identify and drive such topics.
- **We define what Information Security means for the TecAlliance Group**
  We provide guidelines, develop and maintain the Information Security Management System (ISMS).

3 Handling of Information

There is a relationship between the criticality of information and the way it is used. In short, we value the need-to-know-principle and handle information differently according to its classification.

➲ Applicability
Guidelines in this chapter are applicable for the handling of information within TecAlliance and to/from other parties. That explicitly includes information exchange between all sites and all subsidiaries where TecAlliance GmbH owns more than 50% and between those TecAlliance entities and third parties.
➲ Purpose
Purpose of guidelines on how to handle information is to ensure that information is only accessible by parties that are allowed to access it.

3.1 Information Ownership

The information owner is responsible for how information owned by him is handled and by whom. The information owner is determined in this order as the first person being an employee of the TecAlliance Group:

- The individual creating, gathering or digitizing the information
- The individual that acquires the information for use by the company
- The BU Lead in who's responsibility the information is handled
- The EVP in who's responsibility the information is handled
- The CEO of TecAlliance

Information ownership can be delegated within the TecAlliance Group, delegation has to happen explicitly. If you derive your data from information that is already associated with an information owner within TecAlliance, the original ownership remains. You do not become owner of the information in this case.

This definition of information ownership is to be used within the TecAlliance Group. Legal definitions of information ownership may vary across different countries. This definition does not interfere with those definitions, however, if a legal definition differs, it always prevails.

3.2 Classification and Labeling

There are different levels of information based on their confidentiality requirements:

1. Public (e.g. Press announcements, newsletter)

   Public information is any information that is cleared for public distribution by the information owner. Any information that is publicly accessible via the TecAlliance homepage or similar distribution channels can be considered public. Public information does not need any additional means of protection.

2. Internal (e.g. Meeting minutes not including PII, business telephone numbers)

   Information classified "internal" is for internal usage. Forwarding to business partners is allowed when necessary from a business perspective. Any information not marked as "confidential" can be assumed to be internal. You may store internal information unencrypted, printed or otherwise unprotected in places such as a cupboard when inside of a company building. Internal information has to be handled responsibly and according to the decisions of the information owner.

3. Confidential (e.g. Salary information, company secrets)

   Confidential information should be marked confidential in a way that is immediately visible to a viewer (e.g. as part of the header of a web application or as part of the footer of a document). Access has to be restricted technically (e.g. by requiring a login of a user in a named list or by physically locking in case of paper documents). Confidential data has to be encrypted. Confidential information may only be shared with individuals outside the organization on basis of an NDA.

> ➲ Note
>
> We deliberately left out the classification "secret" (which would have higher security needs than confidential information). If you have the need for a higher classification than "confidential", please contact IT Security (security@tecalliance.net), we are happy to hear your requirements and improve our methodology.

The classification should be performed by the information owner based on an estimate of the business impact in case the information is disclosed publicly. If there is a considerably impact, information should be classified as confidential.

Handling **personal data** means dealing with confidential information in most of the cases. For details see

Legal Requirements on page 14.

Login credentials are treated as confidential information regardless of the information they provide access to.

➲ Note

Storing and transmitting data encrypted is not as hard as it sounds. Our notebooks are completely encrypted using Bitlocker with a key stored in the TPM, so everything you store on your local notebook disk is already encrypted. When you store something in the cloud (e.g. Office 365) using TLS, you already transmit it encrypted.

In edge cases you can always find a solution by thinking about the problem. E.g. when you need to transmit something via email to an external party, who is unable to use PGP or S/MIME and does not have a login to a storage you could use, you can still encrypt the data in a ZIP container and tell him the password in a phone call.

3.3 Transfer

Information has to be transferred encrypted, regardless of the classification.

3.4 Clear Desk

Do not leave your confidential information unattended. Lock your screen when leaving your computer. Lock printouts of confidential information when you are not in the room. When you store confidential information on digital volumes make sure they are encrypted in a proper way (e.g. using Bitlocker and a TPM for the key).

➲ Note

From time to time people tend to forget to lock the screen when leaving the room. A friendly reminder of co-workers helps to raise awareness. Also, a timeout of 5 minutes for the automatic screensaver to kick in is considered a good idea.

3.5 Legal Requirements

➲ Purpose

Purpose of this chapter is to fulfil legal requirements concerning Intellectual Property and Data Privacy regulations.

3.5.1 Privacy, GDPR

According to the GDPR, it is legally prohibited for all employees involved in data processing in any form to collect, process, disclose, render accessible or to otherwise use protected personal data for a purpose other than for the purpose associated with the respective lawful fulfilment of a task. Data processing includes the registering, recording, storage, transfer, amendment, deletion, use, collection and blocking of personal data. Misuse of the commissioned data thus also exists if information of which one has become aware in a professional capacity is used for private purposes.

The statutory protection of personal data extends to data stored in files, regardless of the procedure applied during processing. The law fundamentally protects all data pools containing personal data (e.g. registers, data entry forms, punch cards, magnetic tape, microfilm recordings, and similar). Protection also extends to processes through which such data is processed. Furthermore, when data is processed for the company's own purposes by the Accounting department, the principles of proper data processing in terms of proper accounting are to be observed and, when personal data is processed, the special protection of personal data is to observed, even outside of the company.

Every employee is obliged to handle personal data as confidential according to these regulations. This obligation in respect to data secrecy shall also continue after the employment relationship ends.

3.5.2 Keeping of company secrets

All of the developments, constructions, production techniques and business transactions processed in the company and the content of employment contracts outside of one's own are considered company secrets. Every employee is obliged to maintain silence concerning the knowledge and experience gained during the employment relationship as well as facts, company secrets and business secrets of which he has become aware by virtue of his position in the company, and not to render them accessible in any form to third parties, nor also to use them for his own purposes.

All written documents, such as drawings, blueprints, development reports etc. that are accessible to the employee in an official capacity must be handled responsibly and stored securely to prevent unauthorized persons from becoming aware of them. Every employee is obliged to reimburse damage that results from him/her using a company secret without authorization for the purpose of competition or for his/her own use or with the intention of rendering harm to the company or in other cases within a breach of loyalty, or making them accessible in any form to anyone

4 Passwords

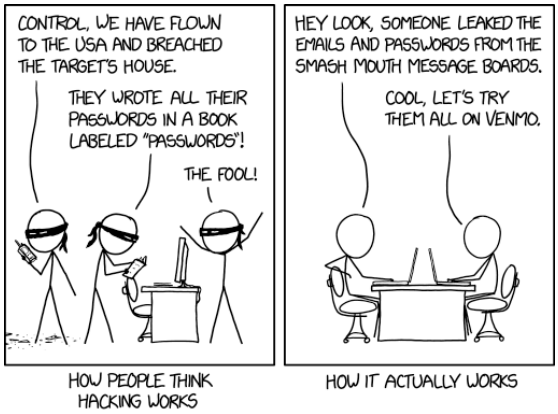
The combination of username and password is used to identify an individual in order to grant or deny access to a resource.

➲ Applicability
Guidelines in this chapter are applicable for handling of passwords by employees of TecAlliance, including all sites and all subsidiaries where TecAlliance GmbH owns more than 50%.
➲ Purpose
Purpose of guidelines on how to handle passwords is to ensure that a system can properly identify an individual in order to grant or deny access to a resource.

4.1 Obligations of users

Do not disclose your password to anybody. Do not store unencrypted. Do not use the same password on multiple sites

➲ Note



(Source: https://xkcd.com/, license: http://creativecommons.org/licenses/by-nc/2.5/)

4.2 Obligations of development and operations

Please see Handling of User Accounts and Passwords on page 25.

4.3 Complexity

Minimum length of a password that is considered reasonably strong is 12 (16 for administrative accounts that can be used to login to a Windows system), including at least three of the following categories:

- Upper case letters
- Lower case letters
- Numbers
- Special characters

Do not repeat the last five passwords and do not use easy to guess password combinations.

Avoid the following password categories:

- Words that can be found in dictionaries, also including variations and additions (e.g. P@$$w0rd11.)
- Passwords that derive in a trivial way from the previous one, e.g. by counters (e.g. Passw.ord1 -> Passw.ord2)
- Simple combinations (e.g. qwertzuiop12)

➲ Note on how attacks work

Attacks against passwords have advanced in the past. Typically, an attacker that performs password guessing tries the following:

- Common Passwords from past breaches (e.g. Sommer2019 or qwertz123)
- Dictionary words in different languages and first/last names (e.g. scraped from Facebook)
- Permutations of the previous, typically:
    - Mixing upper and lower case (e.g. Password -> pAsSword)
    - Replacing characters (e.g. Password -> P@$$w0rd)
    - Adding Numbers and special characters, typically at the end (e.g. Password → Password1!)
    - Combinations of two words/names (e.g. MartinRuf)

Password guessing is typically performed against password hashes (dumped from breaches or Windows domains). Hashes can be calculated from a password, but calculating the password from a hash is practically impossible, so an attacker has to guess.

➲ Hint on remembering complex passwords

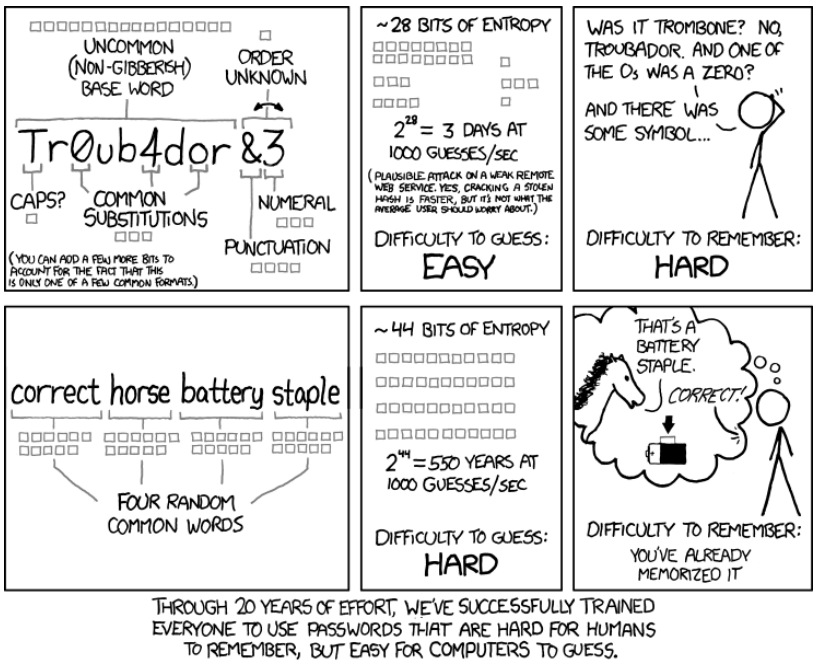
Complex passwords may be hard to remember, so it is a good advice to remember the least amount of passwords possible without using the same password on multiple sites. Please consider using a password manager. A password manager generates random passwords for you and allows you to save them encrypted. This way, you typically reduce the number of complex passwords you have to remember to two (one to log in to your computer, the other one to unlock the password manager).

We recommend using KeePass. You can find KeePass in the Software Center of your corporate notebook. Also consider to put the file where KeePass stores your passwords on OneDrive to make sure they are backed up and you don't loose all your passwords. You can find a detailed installation and usage instruction in the intranet.

There are a few tricks on how to choose a password that is hard to guess, but easy to remember, one of them being:

- Remember a sentence and use the first letter of every word, replacing some with numbers and special characters. Example: "In the morning, I get up and brush my teeth for three minutes" might become "Itm,Iguabmt43m". Do not use sentences that are likely to be used by other individuals as well (e.g. sentences from movies or poems) as they eventually end up in password guessing dictionaries.

Also, there is basic truth in the this comic:



(Source: https://xkcd.com/, license: http://creativecommons.org/licenses/by-nc/2.5/)

4.4 Changing passwords

Passwords have to be changed once a year and whenever there is sneaking suspicion that the password is known to others. Initial passwords have to be changed as soon as possible.

➲ Note

In the past, the common mindset of the industry was to change the password on a regular basis. This was primarily due to the fact that guessing a password is heavily dependent on computation power and an attacker typically had hardware machines calculating hashes all day. Guessing passwords with a reasonable length took some time so the basic concept was that one would change passwords more frequently than an attacker can guess them.

Nowadays, anybody can use parallel cloud computing to guess passwords, so time is not the only relevant factor anymore (money still is, though). And forcing people to change passwords frequently results in weak passwords, because one can assume that there is an easy to remember part of the password that somehow increments used by a reasonable amount of people (e.g. Summer.2020 or MyPassword5!).

On the other hand, not changing the password at all means not giving credit to the fact that there is a constant chance of exposure, from accidentally typing in the password in front of a surveillance camera to a new password pattern becoming common and used against a past breach.

Remembering a new, complex password once a year can be considered doable and is a good trade-off. Also, changing passwords that are included in a breach is absolutely mandatory (though we might not be informed about the majority of breaches).

4.5 Bypassing password protection

➲ Applicability

Guidelines in this chapter are applicable in case password protection has to be bypassed by the company.

➲ Purpose

Purpose of guidelines in this chapter is to regulate access to company data that is protected by user credentials in case the credentials are not available. It should be possible for the company to access all company data, even if the user is not available or forgot his password, but misuse of this possibility in order to gain more privileges should be barred.

The user responsible for the password himself and his superior may request bypassing password protection.

IT-Service may bypass password protection together with a representative from the workers' council and the Data Protection Officer upon request after identity of the requestor and legitimacy of the request was verified. Bypassing password protection includes setting a temporary password that is only provided to the requestor and immediately changed by the requestor.

If the password was bypassed and changed by the superior, the password generated during this process may not be bypassed upon request of the user. In this case, the user responsible for the password has to be informed.

Bypassing password protection requires documenting the following information by IT Service and maintaining the documentation for at least a year:

- Date and time
- Identity of the requestor
- Identity of the individual bypassing the password protection
- Means by which identity of the requestor and legitimacy of the request were verified

5 Handling of IT systems and media

➲ Applicability

Guidelines in this chapter are applicable for all employees of TecAlliance that work with IT systems or media, including all sites and all subsidiaries where TecAlliance GmbH owns more than 50%.

➲ Purpose

Purpose of guidelines in this chapter is to ensure three things:

- Risk for the company created by handling of equipment is not increased by non-company usage
- Leakage of information that may result from improper disposal or accidental loss of equipment is prevented
- Risk of security breaches resulting from running software is balanced with the business purpose of running software

Also, we have to comply with legal regulations.

5.1 Bypassing technical security restrictions

You may bypass technical security restrictions (such as URL filtering) temporarily, if the risk introduced by your bypass does not outweigh the value gained by doing so. You have to inform IT Security (security@tecalliance.net) immediately about every bypass you implement. Depending on the case, IT Security will forward this information to the individual responsible for the security mechanism that is bypassed. You have to remove the bypass if requested by the individual responsible for the security mechanism. You are responsible for any risk introduced or increased by your bypass.

➲ Note

One who is responsible for running a service is also responsible for running it in a secure manner. This usually leads to security restrictions for anybody operating the service (from requiring a password to running anti-virus software). We are a company of IT natives and it is in our nature to make stuff work and overcome technical restrains. This hacking culture is a good thing. When you bypass something and inform about it, then you are basically doing two very valuable things:

- You point out a weakness in the security mechanism (which may lead to a stronger mechanism, may not perfectly fit your agenda, but helps the company stay secure)
- You also point out that the security mechanism restricts you in a way that you perceive as being unproportionally in your specific scenario (assuming you would not bypass the restriction if the risk introduced by your bypass would outweigh the value gained by doing so). This is a very good feedback channel for the rationale of having the restriction in the first place.

5.2 Loss of IT equipment

The loss of company property (especially regarding (electronic) keys, tokens, laptops, smartphones, etc.) is to be reported to IT Operations immediately.

5.3 Returning IT equipment

Company owned IT equipment has to be returned to the company by the employee before his contract ends.

5.4 Inventory

> ➲ Note
>
> The devices of employees are regularly scanned by IT Operations for the software installed on them (automatic inventory taking)

IT Operations has to maintain an inventory of assets they provide and every entity (e.g. Business Unit) has to maintain an inventory of assets that they manage on their own. The inventory has to list every item and the current user(s) of this item (e.g. a notebook and the user of the notebook).

5.5 Installation of software on operational systems

The installation of software on operational IT systems has to be approved by the individual responsible for the IT system in question.

> ➲ Note
>
> Responsible for your notebook usually is a member of IT Operations. If you need to install software on your notebook, either install pre-approved software from the Software Center or contact IT Operations.

5.6 Smartphones

➲ Purpose

The company provides smartphones for business use and also allows limited private usage of the devices. The smartphones have access to central infrastructure (e.g. e-mail system) and therefore, compromised smartphones can be a threat for the company. Additionally, the company has to comply to legal regulations (such as GDPR). Policies on smartphone usage have the purpose of balancing the risk that occurs from private usage with the benefit that is provided to employees and to adhere legal obligations.

The private usage of smartphones owned and provided by the company is allowed, unless it affects company demands. IT Operations manages company owned smartphones, which includes the usage of an MDM[1] system. Corporate IT has to maintain an acceptable level of security[2] and has to ensure that TecAlliance complies to legal regulations (such as GDPR[3]).

➲ Note

Initially, private usage primarily meant making calls while not blowing it out of all proportions. Using the web browser and an app to navigate around is also fine, but compromising company security by private usage (e.g. not having a screen lock and accessing company e-mails) has to be avoided.

Frankly speaking, company interests always beat private interests on a company owned device. TecAlliance tries to provide you the maximum benefit possible, but feel free to buy a private smartphone for private usage and configure it as you like if you do not agree to the way company smartphones are managed.

[1] Mobile Device Management
[2] Same as notebooks, this level is determined by the system owner, who usually is within IT Operations
[3] General Data Protection Regulation (see https://eur-lex.europa.eu/eli/reg/2016/679/oj)

5.7 Telecommuting

> ➲ Note
>
> Telecommuting, including Home Office is quite common within TecAlliance. Only reason why we explicitly mention it is because the ISO27001 requires us to.

Devices used for telecommuting are provided and managed by TecAlliance. The security level of all end user devices have to meet security requirements for telecommuting, which are:

- Full disk encryption where technically possible
- Adequate access protection (see Passwords Passwords)

The employee performing telecommuting has to prevent leakage of information by his surroundings (e.g. by eavesdropping on his screen, notes or printouts).

5.8 Removable Media

Whenever possible, do not use removable media for data transfer. In rare cases, it can be necessary to use removable media. In such cases, ensure the following:

- Do not use media where you do not know the source (e.g. USB drives you find on the floor)
- Make sure you do not expose the data on that media during transportation (e.g. by encryption or guarding it)
- Do not use removable media for confidential information

5.9 Disposal

Confidential information on paper is disposed using special disposal bins located in every office. IT equipment and digital media is collected by IT Operations and handed over to Administration for disposal within the European Economic Area. Outside of the European Economic Area the local branches are responsible for secure disposal of IT equipment and digital media. Unless agreed otherwise with CCS-IT Security, digital media has to be destroyed physically. Verifiable proof that no data has left the company (e.g. disposal protocol referring to the individual piece of hardware) has to be maintained for one year.

> ➲ Note
>
> Back in the days, overwriting media before disposal was common. Nowadays, technology has become much more complex. SSDs and hybrid drives have emerged, where wiping is really hard and secure wiping the media heavily depends on the specific model.
>
> Also, we do not want to rely on encryption alone as this has implications on key management and depends on the drive age.

6 System design

➲ Applicability
Guidelines in this chapter are applicable for the implementation of any combination of physical systems (such as a notebooks), virtual systems (such as a VMs) or applications (such as a web applications or technical services). This explicitly also includes solutions.
➲ Purpose
Purpose of guidelines in this chapter is to ensure that systems are designed, implemented and improved with security in mind during the complete system lifecycle.
➲ Note
The term System describes any combination of physical systems (such as a notebooks), virtual systems (such as a VMs) or applications (such as a web applications or technical services). For a precise definition, refer to the global IT Governance definitions.

There has to be an individual responsible for each IT system. This responsibility has to be documented or derivable from existing documentation.

6.1 Access Control

➲ Note
This chapter is very generic and will be specified in more detail in later releases of this document.

Every individual responsible for a piece of hard-/software, service or solution (“System Owner”) is also responsible for how information is handled within and the access control mechanisms protecting their hard-/software, service or solution.

6.2 Backup

➲ Note
This chapter is very generic and will be specified in more detail in later releases of this document.

Backup mechanisms have to be considered depending on the value of systems and data.

6.3 Cryptography and Key Management

➲ Note
This chapter is very generic and will be specified in more detail in later releases of this document.

Always encrypt communication if technically possible. Do not implement cryptographical functionality on your own, use proven and well-known libraries instead. Protect your private key in a reasonable way. Choose a reasonable lifetime for certificates[4].

6.4 Handling of User Accounts and Passwords

The combination of username and password is used to identify an individual in order to grant or deny access to a resource.

➲ Applicability
Guidelines in this chapter are applicable for development and operations of systems that handle passwords.
➲ Purpose
Purpose of guidelines in this chapter is to prevent leakage, prevent successful password guessing attacks and enforce complexity of passwords.

Access to stored passwords should be prevented. Do not save passwords in clear text. When necessary (e.g. for authentication), only save a salted hash of reasonable strength[5]. Do not include passwords in log files. Do not transmit passwords in clear text.

[4] Two years is considered maximum for TLS server certificates
[5] SHA256 is considered reasonably strong at this point in time.

Technically lock accounts that are not used for an extended timespan[6].

Implement an effective mechanism against password guessing attacks, e.g.:

- Lock accounts for two minutes after three failed login attempts. Entering the password for a locked account must not result in an indicator whether or not the password that was entered is correct.
- Increase the time for each login attempt by factor 2 starting with 0,5 seconds (first attempt takes half a second, second one takes one second, third takes two seconds and so on). Maintain the time individually per account, not per IP address, session or the like.

Enforce password policies described in chapter Passwords (see page 15).

Enforce password change on the first login.

Ensure that accounts are necessary and actively used. To achieve that, a regular check of the last login date is considered reasonable. For TA-accounts of external service providers and partners, this is performed by IT-Operations.

6.4.1 Central Reporting

➲ Purpose

We want to make sure that systems holding authentication material are integrated into offboarding processes and have a decent security level, e.g. regarding the hashing algorithms used.

Every system maintaining more than 15 identities with corresponding authentication credentials (usually usernames and password hashes) has to be reported centrally. For this purpose, Information Security provides a Sharepoint List[7].

➲ Note

Please be aware that responsibility for maintenance of access permission remains with the system owner.

[6] The timespan depends on the usage of your application. For employee AD accounts, 90 days is considered an extended timespan at this point in time.
[7] https://tecalliance.sharepoint.com/sites/InformationSecurity/Lists/Identity Management Systems/AllItems.aspx

6.5 Operating Procedures and Change Management

➲ Note

This chapter is very generic and will be specified in more detail in later releases of this document.

The individual responsible for a piece of hard-/software, service or solution is also responsible for operating procedures and change management in accordance to the business value.

6.6 Acceptance Testing

➲ Note

This chapter is very generic and will be specified in more detail in later releases of this document.

The individual responsible for a piece of hard-/software, service or solution ("System Owner" as described by the global IT governance role definitions) is responsible for acceptance testing in accordance to the value of the system.

6.7 Mandatory Penetration Testing before go-live

➲ Purpose

We want to make the security level of a new system transparent before going live to prevent easy-to-spot-vulnerabilities in new systems.

Every system has to conduct a Penetration Test before going live for the first time. Penetration tests are coordinated (and in most cases also conducted) by Information Security.

➲ Note

Please make our lives a little easier by getting in touch with us at least 3 months in advance.

6.8 Business Continuity / Disaster Recovery Plan

➲ Note
This chapter is very generic and will be specified in more detail in later releases of this document.

The individual responsible for a piece of hard-/software, service or solution ("System Owner" as described by the global IT governance role definitions) has to determine if a formal continuity plan is necessary depending on the continuity requirements of the hard-/software, service or solution. He is also responsible for definition, documentation, implementation and testing of the continuity plan where considered necessary to meet business requirements.

6.9 Logging

➲ Note
Connection to central logging and monitoring facilities might be required once the overall security maturity level of our company is high enough that such a measure would actually result in a security gain.

The individual responsible for a piece of hard-/software, service or solution is also responsible for logging and ensuring a common time synchronization in accordance to business considerations.

6.10 Additional Legal Requirements

➲ Applicability
Guidelines in this chapter are applicable for development of software that processes personally identifiable information (PII) of a natural person.
➲ Purpose
Purpose of guidelines in this chapter is to ensure compliance with legal regulations (including GDPR).

The accountable Product Owner has to inform the Data Privacy Officer as early as possible about every new procedure (solution, application, process) or every change, so that he can check the privacy compliance.

Collect personal information from individuals only for the purposes identified in the provided privacy notice (agreement between PO and Data Privacy Officer), and only to provide the product or service that has been requested or authorized by the PO. In principle no PII data may be recorded in event logs. In the case the Data Privacy Officer of TecAlliance is accepting an exception to this requirement it must be ensured that an evaluation of the log files on a personal level is not possible. Every exception or deviation to this guideline has to be agreed by the Data Privacy Officer of TecAlliance.

7 Risk Management

➲ Applicability
Information Security Risk Management is applicable for every information owner within the TecAlliance Group and for every individual responsible for a piece of hard-/software, service or solution ("System Owner" as described by the global IT governance role definitions).
➲ Purpose
Purpose of this chapter is to be more precise and to clarify roles corresponding to the TecAlliance Risk Management process.

For the process, please refer to the TecAlliance Risk Management processes, IT Security Risks are managed according to company wide regulations.

Estimation of information security risks is performed using the methodology described in this chapter.

7.1 Risk Estimation

Risk is estimated as a financial impact (in Euro) that happens at a certain rate/frequency ("probability per timeframe" – "X times per year"). This value is called "Annual Loss Expectancy" (ALE) throughout this document.

The ALE is the product of:

- The frequency in which the entry point is exploited – this is called "Annual Rate of Occurrence" (ARO) throughout this document. If a risk scenario can occur through multiple potential entry points, the highest ARO is taken to estimate the risk scenario.
- The financial impact in Euro
- Beneficial or unbeneficial factors on the exploitation chain (this tries to answer the question "how likely is it that a successful attack of the entry point results in damage to the company?"). This can also be thought of as a list of preconditions with a certain probability that the condition is met.

Measurement unit is Euro per year, calculation is as follows:

$$ALE = ARO [\times Factors] \times Impact$$

7.1.1 Guessing Probabilities

A probability without a fixed timeframe is calculated as a number between 0 and 1. To translate between natural language and a number a calculation works with, the following table is used:

Probability (Human)	Probability (Number)
Almost impossible	0,03
Highly unlikely	0,1
Unlikely	0,15
Possible	0,2
50 Percent possible	0,5
Likely	0,75
Certain	1

7.1.2 Estimate Annual Rate of Occurrence (ARO)

If it can be estimated directly (e.g. based on statistics) the value in Times per Year is taken.

Examples:

- Once in a year would be an ARO of 1
- Every 5 years would be an ARO of 0,2
- Every week would be an ARO of 52

If it can't be estimated directly, it is estimated based on two questions:

1. Once exposed to the threat, how likely is it that impact occurs (=damage happens)? This is the "Likelihood of Occurrence" that is chosen from the following options:
    a. Almost impossible
    b. Highly unlikely
    c. Unlikely
    d. Possible
    e. 50 Percent possible
    f. Likely
    g. Certain
2. How often is the subject exposed to the threat? This is the "Frequency of Exposure" that is chosen from the following options:
    a. Once in a few years (for the calculation we assume "few" means 5) [=0,2 times/year]
    b. Annually [=1 time/year]
    c. Monthly [=12 times/year]
    d. Weekly [=52 times/year]

After answering both questions, we get the ARO by multiplying[8]

a) the Likelihood of Occurrence from step 1 (value taken by using the transition table above) and

b) the Frequency of Exposure from step 2 (the value in times/year)

7.1.3 Estimate one-time-impact

If possible, the one-time-impact is estimated directly in Euro.

If it is not possible, it is estimated by adding up estimations of at least the following categories:

- Rebuild-Costs of the asset. If parts of the estimation involve effort in PD (person days), a daily rate of 800€/day is assumed.
- Incident Response, meaning how much direct response effort would it cause (those efforts are not paying into rebuilding capabilities, but into limiting the impact)
- Liabilities, e.g. of customers due to outages
- Direct Losses, e.g. damage on other components directly created by the impact
- Lost customer relations, estimation for one year

Cost estimations in risk evaluations are expected to have a high uncertainty.

7.1.4 Mapping to company risk categories

If you need to map it to the TecAlliance company method, do as follows:

- map the ARO to the Probability (multiply by 100 to get a percentage value)
- map the One-Time-Impact to the Damage Class

[8] The methodology is also described in the intranet (it is used for other risk estimations as well) – you can also find a ready-to-use-table there

8 Suppliers

➲ Applicability
Guidelines in this chapter are applicable for the relationship between TecAlliance and its suppliers, including contractual agreements.
➲ Purpose
Purpose of guidelines in this chapter is to ensure that the TecAlliance security level is not lowered by the suppliers we contract and to ensure compliance with legal regulations (including GDPR).

Please also refer to the Purchasing Handbook for details on the purchasing process, including contractual agreements necessary when initiating any business with external suppliers.

8.1 Information Security Requirements

➲ Note
This chapter is very generic and will be specified in more detail in later releases of this document.

The individual coordinating the supplier is responsible for ensuring that the level of a supplier regarding information security is appropriate to the criticality of the information handled by the supplier.

8.2 Legal Requirements

➲ Applicability
Guidelines in this chapter are applicable for development of software that processes personally identifiable information (PII) of a natural person.
➲ Purpose
Purpose of guidelines in this chapter is to ensure compliance with legal regulations (including GDPR).

8.2.1 Compliance with Data Privacy Laws

Every supplier with access to personal identifiable information (PII) is obliged to comply with the European General Data Protection Regulation (GDPR) in the always current version. Prior to processing PII the supplier has to sign a Data Processing Agreement (DPA) and if located outside the European Union the supplier has to meet the requirements pursuant to Art. 44 ff. GDPR (EU standard model contract, adequacy decision of the EU Commission, or the EU-US Privacy Shield).

The suppliers have to impose such obligations on its staff and other persons involved in handling of TecAlliance data.

The supplier and any person acting under the authority of the supplier, who has access to personal data, have to process those data in accordance with the principles set out in Art. 5 of the GDPR. In particular the supplier and any person acting under the authority of the supplier shall not process those data except on instructions from TecAlliance (Art. 29 GDPR) and the supplier shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR).

The supplier has to defend, indemnify and hold harmless TecAlliance from and against any and all third-party claims, suits and actions and related damages, losses and expenses (including, without limitation, reasonable attorneys' fees) to the extend arising directly or indirectly out of or resulting from Supplier's non-compliance with the GDPR, its staff and other persons involved in the handling of TecAlliance data.

9 Incident Handling

If you are in an incident situation right now, contact

CSIRT@tecalliance.net

Someone from this group will guide you through the incident handling.

➲ Applicability
Guidelines in this chapter are applicable in case of an incident regarding data privacy or information security.
➲ Purpose
Purpose of guidelines in this chapter is to ensure that incidents are handled in a proper way, to reduce the frequency and damage of incidents that occur and to comply with legal regulations (including GDPR).
➲ Note
If in doubt, always contact IT Security (security@tecalliance.net)

9.1 Initiating Incident Handling

An **Information Security Incident** happened when confidentiality, integrity or availability of our information is affected or when an outside actor has significant control over IT systems of TecAlliance. That can involve extracting information that is not supposed to be extracted, modifying the system behavior in a non-pleasant way, or making systems unavailable for what they are supposed to do.

A **Data Privacy Incident** happened when personal identifiable information (PII) gets available to a broader audience than allowed. That includes both data becoming publicly accessible (classical breach) and PII being (accidentally) forwarded to individuals that are not allowed to see it. When any employee has the suspicion that a data privacy incident has occurred, he has to inform both the information owner, who is responsible for the incident handling, and the Data Privacy Officer (CorporatePrivacy@TecAlliance.net).

When any employee has the suspicion that an incident has occurred, he has to immediately inform the CSIRT team (CSIRT@tecalliance.net). One of the members of the CSIRT team will take over the lead in incident handling and becomes the Task Force Lead.

9.2 Task Force

The task force lead creates the task force by involving additional individuals to the incident handling.

The task force has to include the Data Privacy Officer in case of a Data Privacy Incident. Other than that it is up to the task force lead to decide who is included in the dialogue. It is recommended to include staff with technical knowledge about the systems affected and the IT Security Officer, though.

Within the task force, the situation and next steps are discussed and the approach is decided, which includes:

- How the system state is preserved (if applicable). Depending on the case and the technology behind, measures how to secure evidence before starting technical investigations should be discussed.
- How the analysis is performed (offline, online, onsite, offsite, inhouse, by a consulting company, …)
- Which steps are taken to prevent further damage
- Whom to contact at which point in time (communications, authorities, legal, …)

If the task force cannot agree on one approach, the task force lead decides.

It is recommended to meet in online meetings in reasonable intervals and to decide about the next meeting date at the end of each meeting. This way, every member of the task force is informed about the current state of activities.

9.3 Postprocessing

After the analysis is finished, the task force decides how and how long analysis results, documentation and collected evidence is retained (if applicable).

The task force lead is responsible for documenting the incident. The documentation should be done in the Incident Handling Confluence space and should include at least:

- How the incident was detected
- Who was involved in the incident handling
- Which steps were decided at what point in time

The incident documentation is used to have regular lesson's learnt meetings within the CSIRT team.

10 Internal Audits

➲ Applicability
This chapter is applicable for every Information Owner and every individual responsible for a piece of hard-/software, service or solution ("System Owner" as described by the global IT governance role definitions) in a situation where an internal audit is conducted.
➲ Purpose
Purpose of this chapter is to regulate internal audits in a way that both audit efforts and business impact is reduced while maintaining a reasonable information value of the audit results.
➲ Note
This chapter is very generic and will be specified in more detail in later releases of this document.

Internal Audits regarding Data Privacy are conducted on a regular basis. Questions of the Data Privacy Officer have to be answered truthfully and in a timely manner.

Tests of systems during audits need to be planned and arranged by the auditor to reduce impact on business processes.