Information Security and Privacy at TecAlliance

2021-03-25

TecAlliance GmbH
Steinheilstrasse 10
D-85737 Ismaning
Germany

1 About this document

This document describes how Information Security is handled at TecAlliance. It is meant as an information to customers interested in learning about how we handle information security and to those that seek answers to compliance questionnaires.

2 Compliance Landscape

Our statements concerning privacy are publicly accessible and describe how we handle privacy at TecAlliance. Additionally, our guideline “Information Security Handbook (ISH)” describes how we handle Information Security at TecAlliance.

Of course, TecAlliance complies with applicable legal regulations, including those derived from the General Data Protection Regulation of the European Union (GDPR).

2.1 Certifications

TecAlliance is ISO9001 certified.

As of now, TecAlliance does not hold ISMS specific certifications, such as ISO27001, TISAX or SOC.

Information Security and Privacy personnel does hold certifications verifying their relevant skills. Certificates are available on request.

2.2 Audits

Internal Audits regarding Privacy and Information Security are performed on a regular basis. Additionally, ISO9001 audits are conducted by an external, independent party.

You may conduct audits and technical tests (e.g. Penetration Tests) of our services and infrastructure under certain conditions. Conditions are:

- Time and scope of the audit/test is agreed and coordinated with TecAlliance in advance
- Results are shared with TecAlliance
- Depending on the effort on TecAlliance side, additional charges may apply

3 People and Organization

TecAlliance is organized in Business Units and central entities. Business Units are responsible for products and services that are delivered to our customers. Central entities manage common tasks such as financial topics, human resources and IT.

3.1 Information Security Responsibility within TecAlliance

There is a central Information Security department within TecAlliance that takes responsibility for global information security topics. Responsibility for software products and services of TecAlliance – including responsibility for information security aspects – is located within the Business Units.

3.2 Human Resources

Individuals working for TecAlliance have a valid contract including obligation to privacy and confidentiality. There are procedures in place that ensure the invalidation of login credentials once an employee leaves the company. There is no general background screening in place, but there are specific positions in some areas that require background screening.

All employees of TecAlliance are obliged to confidentiality by the employment contract. Additional contracts exist for individuals with extended access to information.

3.3 Trainings

All employees of TecAlliance are trained in both information security and privacy topics on a regular basis. Trainings are mandatory and participation is documented. Additionally, awareness campaigns are conducted.

4 Information Security Process Landscape

4.1 Information Classification

Information is classified and handled according to three different levels of confidentiality: Public, Internal and Confidential. Information that is not labelled is considered internal information.

Independent of classification, information is handled according to the Need-to-Know Principle.

4.2 Partners, Visitors and Subcontractors

There is a process in place that ensures that partners and subcontractors do meet an adequate level of privacy and information security. Additional non-disclosure agreements and privacy related contract additions are arranged where necessary.

4.3 Software installations

There is a central software purchasing and installation process. Employees of TecAlliance do not have an administrative account by default. Installed software is monitored centrally.

4.4 Application Security

There is no TecAlliance-wide Software Development Lifecycle (SDLC) in place. All aspects of information security in the development lifecycle are managed by the corresponding development team, including test-/development-/staging systems and maintenance windows.

Depending on the information security requirement of the specific solution, additional measures are in place. These include:

- Static Code Analysis
- DDoS protection services
- Web Application Firewalls
- Penetration Tests
- Anomaly Alerting

There are coding guidelines in place.

4.5 Incident Management

There are defined processes for privacy and information security incidents. The processes include a lessons learnt and relevant contacts to authorities as well as information to affected customers and individuals where necessary.

Incident Handling is done on a Task Force approach, including relevant stakeholders per incident. There is a central group of incident handlers originating from different departments that coordinate incident handling. The group meets in regular intervals to discuss past incidents and review procedures and provides response to a central contact point within TecAlliance for incident handling. Currently, there is active detection of selected information security components that may lead to incident handling when assessed being critical enough (e.g. Malware alerts).

Critical incidents are actively reported to management. Either way, the documentation of incidents is accessible to all employees of TecAlliance.

5 Technological Security

5.1 Password Policy

Password policy within TecAlliance is at least 12 characters (16 for administrative accounts) and three out of four categories. Passwords are changed on a yearly basis. Technical measures to prevent brute-force-attacks are mandatory.

5.2 Multi Factor Authentication

Multi Factor Authentication (MFA) is implemented for Virtual Private Network (VPN) Access and Office 365.

5.3 Physical access to facilities

Physical access to facilities within Europe is restricted by electronic access tokens and local receptionists. Access to specific areas (e.g. server rooms) is restricted.

The access restriction remains functional when infrastructure fails (e.g. during a power outage).

5.4 Devices and Media

In general, devices of TecAlliance employees are mobile devices. Notebooks are encrypted using state of the art technology and smartphones are managed using state of the art mobile device management software.

All notebooks are equipped with a malware protection tool. E-Mails are checked for malware. Servers are partially equipped with malware protection tools. Identified malware is quarantined and alerting is triggered. Malware signatures are kept up-to-date.

There are guidelines in place that regulate the usage and disposal of media. IT equipment is disposed in a secure manner to ensure no data leaves the company on devices that are disposed.

There is an asset management process supported by asset management software in place. IT equipment of TecAlliance is documented, every piece of IT equipment has a responsible individual (“owner”) assigned.

5.5 Backup

Backups are handled according to the risk estimation of the responsible employee and thus differently across the organization.

5.6 Logging

Logs are handled according to the risk estimation of the responsible employee and thus differently across the organization.

5.7 Network Security

Access to the company network is provided either physically or using a Virtual Private Network (VPN) access. There are firewalls and there is an Intrusion Detection and Prevention System in place. Additionally, there are DDoS protection mechanisms and Web Application Firewalls in place depending on the solution.

Logs of firewalls and intrusion detection system are reviewed on a regular basis additional to alerting.

5.8 Vulnerability Scanning

Vulnerability scans of externally accessible infrastructure components are conducted on a bi-weekly basis. The internal network is scanned monthly.

There is a publicly known contact point to report vulnerabilities[1]. There is no Bug Bounty program in place. TecAlliance did not publicly disclose vulnerabilities so far.

5.9 Penetration Tests

Penetration Tests are performed both using internal penetration testers and by external companies. Penetration Tests are performed regularly and on demand. Vulnerabilities are rated and prioritized using CVSS[2].

[1] https://www.tecalliance.net/.well-known/security.txt
[2] https://www.first.org/cvss/

6 Contacts

For information security topics please contact

Security@TecAlliance.net

For privacy topics please contact

CorporatePrivacy@TecAlliance.net