Security Concept

Details on access and access control

November 2024

Content

1 General

This document summarizes relevant information from AEB's “Security Concept” and provides more details. You can find the Security Concept in the AEB Trust Center (https://www.aeb.com/en/trust-center).

2 Principles

Applications, data, devices, networks, and accounts are individually protected against unauthorized access wherever they are located.

2.1 Roles concept

AEB grants customers, employees, and partners access using central user repositories and a role-based security model. This ensures that users can access only the applications and environments for which they are actually authorized.

Accounts are summarized in security groups. It is not the individual account object which is granted access, but it is always the group objects.

2.1.1 Application to employee accounts

The creation of new accounts/logins for employees and the approval of authorizations and the assignment to roles are only granted upon written request and upon the respective approval according to the “need-to-know” principle (see processes in the appendix).

2.1.2 Application to customer accounts

An initial customer account is created for customers and included in all customer-specific administrator groups.

The customer is then responsible for creating new accounts/logins and assigning them to the relevant security groups.

2.2 User accounts

All employees, customer contacts, and partners are provided with a personalized access code and password. Only this access may be used.

2.2.1 Principles for passwords

Account holders are responsible for passwords.

The usual principles apply to all passwords. These include “difficult to guess”, “does not contain personal information”, “is not written down” (except in a dedicated password safe).

These regulations apply uniformly to the following account types: Employees, customers, and services.

Wherever possible, a second factor is enforced.

Passwords must consist of at least 11 characters.

Passwords must include at least three of the following four characteristics

- at least one numeral
- at least one special character (non-alphanumeric character)
- at least one capital letter and
- at least one lower-case letter

A central guideline automatically enforces this.

2.2.2 Password rotation

For accounts of AEB employees

For these accounts, AEB follows the latest findings and recommendations of NIST or BSI, for example, not to allow password rotation to increase security.

For customer accounts

The AEB platform (nXt) does not provide for password rotation. This corresponds to the findings and recommendations of NIST or BSI, for example.

In all other applications, customers decide on the use of password rotation; both variants are possible, but AEB recommends not using password rotation.

2.2.3 Biometric recognition

Biometric recognition, if it cannot be used generally for a global account but for logging in to exactly one device, is a possible alternative for AEB employees. These devices are also protected accordingly. For example, through enforceable rules for login and remote wipe (e.g. through MAM/MDM on current Android, iOS, or MacOS devices provided by AEB).

We therefore allow login via fingerprint and modern facial recognition (with deep scan) explicitly for

- Windows Hello for AEB notebooks with at least Windows 11
- Current Mac OS on AEB Mac devices
- Apple iOS/iPadOS devices
- Android smartphones

This is enforced as follows (in addition to other rules):

- Remote wipe can be triggered manually by an administrator
- Remote wipe after 10 wrong attempts
- For Windows 11 Hello additionally:
    - a 7-digit pin

Biometric recognition is not allowed for privileged accounts

2.2.4 Multi-factor authentication

Active for all AEB employees and partners.

Possible for customers in the AEB Private Cloud or with the help of a user repository coupling (see below).

2.2.5 User repository or domain coupling

A connection to external user repositories, a customer domain, or the use of LDAP directories is possible in the AEB Private Cloud.

2.2.6 Automatic deletion/deactivation of accounts

An account will be deactivated/blocked after 180 days of inactivity

An account will be deleted after 360 days of inactivity

An unconfirmed account that an AEB employee creates for someone will be deleted after 30 days

An unconfirmed account that you create for yourself will be deleted after 7 days

2.3 Administrative/privileged roles

Users with special administrative rights or privileges are also consolidated in appropriate security groups, where they are subject to the groups' processes and approvals.

Those responsible for these roles are usually IT managers, the IT security manager, or company management.

For particularly privileged rights (firewall access, admin portals, SSH keys passphrase, etc.), users must use a special, personalized administration account. The "normal" user account will not be granted these rights / cannot be assigned to the respective roles.

2.3.1 Principles for passwords of privileged accounts

The usual principles apply to all passwords. These include "difficult to guess", "does not contain personal information", "is not written down" (except in a dedicated password safe).

Passwords must have at least 14 (fourteen) characters

Passwords must meet at least three of the following four criteria:

- At least one upper-case letter
- At least one lower-case letter
- At least one numeral
- At least one special character (non-alphanumeric character)

It is especially important to note that the last 24 passwords may not be reused.

Wherever possible, a second factor is enforced.

3 Entry in detail

The AEB buildings are divided into security zones. There are

- public areas
- private areas
- specially protected areas

The details, which apply to all AEB locations, can be found below. For the HQ, more site-specific details are provided separately. For all other locations, the location-specific characteristics can be found under the respective "on-site security measures..." (see below) In general, however, we treat locations as "private areas" with the exception of the HQ.

3.1 Public area

This area is intended for all guests (customers, partners, speakers,...).

During office hours this area is open and accessible without authentication.

Employees or their accompanying guests can access this area also outside the regular office hours, for example using the corresponding personalized transponder.

At the HQ:

The opening hours of the main entrance door (manual control) are Monday to Friday between 8:00 a.m. and 5:00 p.m.. The opening hours of the underground parking garage differ, entry 7:00 a.m. to 10:00 a.m. and exit 3:00 p.m. to 4:50 p.m.. The gates are closed outside these times.

Access outside opening hours is only possible with authorized transponders. This area is also monitored by a security service.

Parts of the area are under video surveillance and marked accordingly, see Video surveillance Stuttgart. The area includes the outdoor facilities and the underground parking garage except for the "specially protected areas" listed below.

3.2 Private area

This area is only accessible for employees, accompanied and supervised guests, and a few partners.

Entry is only possible with a special “key” (transponder).

At the HQ:

Access via lifts and stairs is only possible with an authorized transponder. This transponder is handed over to employees and selected partners based on their roles. ISO 27001-certified processes ensure that only authorized persons have an authorized transponder.

All entry authorizations are programmed via the locking system.

This area includes all upper floors except for the "specially protected areas" mentioned below.

3.3 Specially protected areas

Specially protected areas are areas where

- data requiring a high level of protection/data with analysis of the need for protection is kept
- activities take place that require particular roles that are specially trained.

This includes rooms in which customer applications run, which host network or security facilities, or facilities important for the building technology, or which are particularly required to be protected due to other reasons.

They include, inter alia:

- Data centers
- Archive
- all network distributors
- Rooms with employee files or accounting data
- Rooms for technical infrastructure (energy supply and safety equipment

Access is only granted to the relevant roles and therefore coded to their personalized transponders and usually complemented with a further secret (e.g. pin code), i.e. only IT administrators have access to the data centers, for example.

All entry authorizations are programmed via the locking system.

4 Access in detail

4.1 Basic information

Due to network and application protection mechanisms (e.g. next generation firewall), it is ensured that only permitted relations can be established.

Due to the security concepts in the networks, it is ensured that access is granted only to authorized persons.

There is a password guideline in place, which is enforced upon all accounts (see above).

Three factors are required for the employees' and partners' access:

1. Login name
2. Password
3. Additional secret (e.g. onetime password, transponder, certificate, etc.)

Access by AEB employees to customer resources is made either by using two factors (login name and password) or three factors (see above) depending on what is requested by the customer.

Access by customers to their resources provided by AEB is normally made by using two factors. If requested by the customer, three factors are also possible (see above).

The above and all processes concerning access control are ISO 27001 certified.

4.1.1 Details about the usual case "AEB network"

Based on a variety of criteria, devices which want to access AEB networks are moved automatically to specific networks.

Special rules apply within the networks.

For the networks, possible relations are documented in the central Rights Management.

4.1.2 Details about the special case "Remote access" (e.g. home office)

Remote access to customer data/applications cannot be made directly.

Employees must always first authenticate themselves in the AEB network with three factors (one account and two secrets). From there, they can open further access points to the corresponding resources and thus indirectly access them.

All security mechanisms of the AEB networks are therefore also effective for remote access.

4.1.3 Details about applications

The rules who is to get which access to an application are defined by the respective application manager together with the role manager, security, and the Data Protection Officer.

Within the applications, access is also controlled by the role concept. An SSO can be integrated into various applications using the central user repository.

4.2 Encryption

Access to AEB applications is always encrypted.

4.3 Logging

Each and every access to AEB applications and applications containing customer data is logged.

The above and all processes concerning access control are ISO 27001 certified.

5 Appendix – Processes

5.1 Basics

All processes are subject to an internal audit taking place at a regular basis as well as to the ISO 27001 audit taking place annually.

Customers can request a summary of the audit or can agree for their own audits with AEB.

5.2 Processes

5.2.1 New users

Triggers for this process

- Request by the HR team as part of the onboarding process

Process for AEB employees

- By entering the data in the HR system, the user account is created automatically and enabled on the date of entry.
- The rights must be applied for separately for employees (see "New role assignment").

5.2.2 New role assignment

Triggers for this process

- Request for role transfer
- Creation of a new role
- Request for certain rights
- Employee already fulfills the role and is therefore assigned it

Process for AEB employees

- Request is sent to the role managers
- Role managers
  - check whether the employees can be assigned the role and whether the employees meet the necessary requirements;
  - clarify with the employees whether they want to take over the role together with the associated responsibilities.
- In case of approval: The employees are assigned the role and automatically get the associated rights
- In case of rejection: The employees are informed about the rejection and the reasons for it

5.2.3 Relinquish a role

Triggers for this process

- Request for relinquishing roles/rights by the user
- Request for relinquishing roles/rights by a third person

Process for employees

- Request is sent to the role managers
- The role managers
  - clarify with the persons who initiated the request as to why the user is to/wants to relinquish the role/rights;
  - clarify with the employees as to whether the employees want to relinquish the role and the associated responsibilities and inform the employees that this is going to happen now.
- In case of approval: The employees are removed from the role and automatically lose the associated rights
- In case of rejection: The employees are informed about the rejection and the reasons for it

5.2.4 Deactivating users

Triggers for this process

- AEB employees leaving AEB

Process for employees

- In case of "imminent danger" the account can be deactivated immediately by the person processing the request. Afterwards, the request is forwarded to the HR team together with a corresponding note.
- Otherwise, the request is forwarded to the HR team.
- If the employee leaves the company, the account is deactivated automatically at the end of the last working day (maintained in the HR system).
- The HR team has the possibility of setting an identifier "Lock network access" in the HR system. As soon as this identifier is set, the user's account is immediately deactivated.

5.2.5 Regular checks

Triggers for this process

- Regular (at least annual) routines of the role manager and application managers
- Annual inventory of the system management‘s rights in the domain
- Regular employee reviews

Process for employees

- Role managers and line managers check the assignments of employees to roles at a regular basis (at least annually) and, if needed, will initiate one of the above-mentioned processes (e.g. employee relinquishes role).
- Role managers and application managers check the assignment of roles to rights at a regular basis (at least annually) and, if needed, will adjust the assignments of roles and rights.

Triggers initiating this for customers

- Automatic routines taking place at a regular basis

Process for customers

All accounts are checked every day:

- An account will be deactivated/blocked after 180 days of inactivity
- An account will be deleted after 360 days of inactivity
- An unconfirmed account that an AEB employee creates for someone will be deleted after 30 days
- An unconfirmed account that you create for yourself will be deleted after 7 days