IT Security Policy

1 Policy

This is the IT Security Policy of BEWO ApS. It includes a description of the overall information security policy, the chosen area of application and the principles behind the security level implemented, as well as general guidelines for operations.

1.1 Introduction

BEWO ApS IT Security Policy sets the framework for the guidelines for the handling of BEWO ApS IT Security Policy. Herby establishing a foundation for the daily work regarding IT Security in BEWO ApS.

BEWO ApS IT Security Policy is based on:

- Commonly accepted practices and policies for information security.
- All relevant rules, laws, guidelines and contracts related to BEWO ApS business area, GDPR, the Danish Marketing Practices Act and labor market agreements.

1.2 Scope

The IT Security Policy includes development, delivery and servicing of solutions/products for BEWO ApS customers, i.e. all of BEWO ApS and all of BEWO ApS activities.

1.3 Goal

BEWO ApS carries out all necessary activities to ensure:

- **Availability**: That BEWO ApS's business systems are available 24/7 and that an IT contingency plan is maintained. This is ensure with the use of backup as an example.
- **Integrity:** That through management and manual inspections/controls of work processes, a reliable and correct function of the IT systems with a reliable data foundation is achieved.
- **Confidentiality:** That BEWO ApS information, hereunder personal data and customer data in the possession of BEWO ApS, only are available to the intended persons in the way that it was intended.

BEWO ApS asseses the risk to its business critical information and other information assets on a yearly basis. Reassesment is also triggered by the following events; changes in threaths, new projects, IT aqcuisitions, as well as in relation to breaches of security.

The objective is that sufficient and documented security is balanced with the desire for an appropriate and user-friendly use of IT, so that employees and customers can carry out their tasks in an optimal way.

BEWO ApS carries out the activities that are necessary to keep employees informed about IT security and about their responsibility towards the company's information and systems (awareness).

1.4 Responsibility

The management is responsible for the day-to-day management of BEWO ApS IT security.

If an employee discovers threats to, or a breach of, information security, or suspects it, they must immediately inform management of this. Ultimately, it is the person responsible for the day-to-day management of information security who must be notified.

Employees who break BEWO ApS's information security policy will be met with the measures prescribed by BEWO ApS' personnel policy.

1.5 Review

BEWO ApS measures, assesses and follows up on information security in the following way:

- Ongoing follow-up of incidents within IT security.
- Ongoing assessments of security aspects in connection with new projects, acquisitions and changes.
- Annual reviews of the risk assessments.
- Implementation of internal controls (audits) of information security in BEWO ApS.

Based on this, the management reviews and reassesses the IT security policy once a year (review).

2 Guidelines for Operations

2.1 Access Control

Rights and access to systems are only granted where there is a business need. The person responsible for a system or the relevant information decides who should have access to the system and/or information. The IT-responsible then assigns the rights based on these decisions.

Servers and computers owned and/operated by BEWO ApS are protected with password and up-to-date antivirus programs and local firewalls.

Laptops with business data, hereunder personal data, are additionally protected with encryption (see section 2.2).

Password management is handled in Azure AD and follows Best Practice – minimum 8 characters, combination of upper/lowercase letters, as well as numbers and special characters. Passwords for third-party systems and password-sharing is managed with a Password Manager. In this case the Password Manager of choice is Bitwarden.

BEWO ApS's other portable devices (mobilephone and tablets) are protected with pin of at least 6 characters.

BEWO ApS's physical premises are secured with an access system. The person responsible for an area decides who should have access to what.

BEWO ApS's critcal it-infrastruktur, hereunder servers and databases, are hosting in the cloud at Microsoft Azure in the Azure Region *North Europe* (Ireland).

Checks and Controls:

The person responsible for a system or the relevant information reviews the assigned rights once a year to check that they are still valid and that there is a business need. Employees' access to the physical premises is also controlled.

2.2 Information and Assets

BEWO ApS information is found on IT assets such as PCs, servers, tablets, smartphones, USB keys, cloud storage and the like, and possibly also CD-ROMs and backup tapes, etc. The IT Security Policy requires that BEWO ApS information is protected in cases of loss, theft, copying, etc.

Encryption of the company's information is supported by a restriction on which persons are given rights to read, correct or delete information. See section on Access Control.

Employees of BEWO ApS are generally not allowed to store company-related data in a cloud storage, such as Dropbox, unless this is made available by BEWO ApS, or approved by BEWO ApS management for company use. If there is an urgent need to store company-related data in an unapproved cloud storage, it is the employee's responsibility to ensure that data is encrypted.

2.3 Documentation

The BEWO ApS IT Security Policy and other guidelines and instructions are available on the BEWO ApS's shared drive.

The day-to-day responsible for managing BEWO ApS's IT security documents risk assessments, incidents, etc. in a catalog on the shared drive, where access is limited to the relevant people.

Checks and Controls:

These documents are maintained by the day-to-day responsible for BEWO ApS's IT security.

2.4 Reliability

BEWO ApS systems and information are backed up so that they can be recreated after a breakdown. This is done at appropriate intervals to minimize the amount of data potentially lost. Backup data is stored in a way that ensures that data is not lost by e.g. physical damage to a server or server room, and that unauthorized persons cannot gain access to confidential or critical data by accessing the backup.

Logging of activities is switched on in BEWO ApS systems, and where there is personal data, access and attempts to access the individual information are also logged.

Critical updates are installed as soon as possible, and other updates periodically.

Changes follow a process of structured tests of the solutions before the change a put in operation. Changes to critical systems takes place as far as possible in planned service windows, to avoid any errors that will affect availability.

BEWO ApS maintains functional separation where possible. As a minimum, it is required that another person, e.g. one from the management, participates in approval of major changes and when assigning administrator rights.

Checks and Controls:

Every six months an exercise is held to ensure that a given backup can be recreated on a similar system and that the functionality is then as expected.

2.5 Classification

BEWO ApS uses the following classification of information:

Public – can be seen and accessed by anyone.

Confidential – can be seen and accessed by anyone in BEWO ApS and by specific customers/partners.

Internal – can only be seen and accessed by someone in BEWO ApS.

Secret – can only be seen and accessed by a small group of people with a specific business purpose.

Information classified by anythin other than Public must be marked as such, including on paper, in email and on the frontpage of documents.

Information classified as Secret must not be send over unencrypted connections or with unencrypted email.

2.6 Communications Security

BEWO ApS's internal network is protected with a firewall that regulates and logs the traffic between BEWO ApS's internal network and BEWO ApS's telecommunications/internet provider (Internet Service Provider, ISP) (the Internet), so that only permitted traffic passes through.

Firewall rules are as far as possible configured according to PCI compliance, which means that only the necessary services are opened and only between relevant network segments, and that rules are defined for both incoming and outgoing network traffic.

All incoming e-mails received by the BEWO ApS’s mail system are scanned for unsafe links to external websites and for potential phishing e-mails. In addition, attached files are scanned for viruses and other malware.

All external access to BEWO ApS’s network and systems is established with encrypted (VPN) connections. The BEWO ApS website and web services use https encryption based on Transport Layer Security (TLS), just as the mail server also handles TLS.

Access to other servers/services and BEWO ApS's internal network is via client encryption protected by 2-factor authentication.

Transfer of, or access to, BEWO ApS’s information to/from external business partners or authorities may only take place in agreement with these, based on the classification of the information, including cases where encryption is used.

PCs and mobile devices that connect to the company's network and systems externally must comply with the company's guidelines. This also applies to employees' own PCs and mobile devices (Bring Your Own Device, BYOD).

2.7 Supplier Management and Outsourcing

Suppliers who are responsible for the operation of BEWO ApS’s IT infrastructure (outsourcing) must comply with BEWO ApS’s requirements for IT security.

Checks and Controls:

There must be an agreement, and if necessary also a data processing agreement, which meets the requirements of the Data Protection Act.

2.8 Employee Safety and Awareness

In relation to job advertisements/appointments, the day-to-day/individual manager assesses whether there are special security requirements, including whether, for example, it is necessary to ask to see a criminal record/child certificate.

As part of the employment procedure, but at the latest on the first day of work, the new employee is informed about confidentiality and other security requirements.

Via awareness training, it is ensured that new employees and all users have the necessary IT expertise, including those who do not have IT training, as well as good security behavior, for example with regard to access to information. This also applies when an employee changes roles in the company. It is the daily/individual manager's responsibility that this happens.

When an employee leaves the company, the individual manager makes that person aware that the confidentiality also applies after termination of employment.

2.9 Security Incidents and IT Preparedness

If an employee discovers threats to, or breaches of, information security, or suspects it, they must immediately inform the appropriate person about this.

The person responsible for the day-to-day management of BEWO ApS’s information security makes an assessment of the reported security incidents as soon as possible after they have been reported.

In the case of incidents involving personal data, BEWO ApS’s procedures are activated for this.

When the incident has been dealt with, it is assessed whether the case can be closed or whether the current risk assessment needs to be updated, which requires new security measures.

The person responsible for the day-to-day management of information security reports on major security incidents in relation to management's annual review.

If external parties are affected by security incidents at BEWO ApS, the day-to-day management is responsible for any communication with affected parties.

3 Approval

This policy was adopted by BEWO ApS management on 11th of October 2023

Jacob Bruun Co-founder & CTO