IT SECURITY POLICY

Pleaz ApS

Last updated on 21 August2024

1. BACKGROUND

1.1 This IT security policy (the ”IT Policy”) has been prepared by the management in order to secure and protect the company’s trade secrets and data relating to identified or identifiable persons (collectively ”Critical Data”).

1.2 The IT Policy describes and determines the key elements of the level of security.

1.3 As an employee, you are required to engage in and comply with the content. All questions, reporting, etc. regarding the IT Policy shall be addressed to management.

2. PERSONAL DATA

2.1 The IT Policy applies to any electronic and manual processing of data relating to identified or identifiable natural persons (”Personal Data”) among our employees, customers, suppliers, etc. pursuant to Regulation (EU) 2016/679 (the ”General Data Protection Regulation”).

2.2 Personal Data” means any category of data that allows you or any third party to identify a natural person. For example, Personal Data may be name, email address and user number/identifier.

2.3 Processing means an activity relating to Personal Data, including for example collecting, recording, organizing, storing, hosting, altering, downloading, transferring, disclosing, or deleting.

3. TRADE SECRETS

3.1 The IT Policy also applies to the company’s trade secrets (”Trade Secrets”) pursuant to Act number 309 of 25 April 2018 (“Danish Trade Secrets Act”), which implements the EU Directive (EU) 2016/943.

3.2 Trade Secrets shall mean any piece of information which:

a) is secret in the sense that it is not known in its entirety or in its exact design or composition or is not readily available to anyone but the company,

b) represents a commercial value because it is secret, and

c) is protected by the company against disclosure.

3.3 Examples of Trade Secrets include patents, customer databases, supplier databases, strategic plans, market analyses, accounting issues, price calculation methods, purchase prices, employee wages, know-how, etc.

4. RISK ANALYSIS

4.1 At any time, the company wants to protect Critical Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure and access.

4.2 The technical and organizational measures have been determined in consideration of the risks involved in the processing of Critical Data.

4.3 It is the responsibility of Chief Product Officer to undertake a more detailed risk assessment to the extent that the circumstances so require.

5. TECHNICAL MEASURES

5.1 All internal systems are as a minimum measure protected by the items on the following list, which is regularly updated to a state-of-the-art technical level of security:

a) Firewall

b) Backup and restore procedure

c) Encryption (https:/)

d) Network segmentation

e) System surveillance

f) Internal administration of system rights

5.2 The Chief Product Officer is required to keep a record of the details of the above, including, for example, names of subcontractors, software versions, backup structure, and encryption standards.

6. ORGANIZATIONAL MEASURES

6.1 The company’s organizational measures include the following general measures:

a) Access control, including the use of password for login on our IT systems

b) Rights management ensuring that only relevant employees have access to Critical Data

6.2 The Chief Product Officer is required to keep a record of the details of the above, including, for example, a description of the requirements for passwords and specific information about the rights management.

7. PHYSICAL MEASURES

7.1 In order to avoid personal data breach due to physical conditions, the following physical measures have been implemented:

a) Access to the company's office requires personal key outside normal office hours

b) The office is locked outside normal office hours

c) No physical employee files exist

8. USE OF SUBCONTRACTORS

8.1 Use of subcontractors in connection with the processing of Critical Data always requires specific approval from Chief Product Officer.

8.2 Subcontractor means a legal or natural person, who, in connection with the performance of services for us, is granted access to Critical Data. It may be an IT provider, such as a cloud service, or a consultant. The approval procedure applies both when Critical Data are transmitted to the subcontractor and when the subcontractor gains access to the company's systems.

8.3 At any time, the use of subcontractors requires that strict confidentiality be imposed on the subcontractor or that the subcontractor is subject to a statutory duty of confidentiality (e.g. lawyers and accountants).

8.4 All agreements with subcontractors, who are processing Personal Data, require a data processing agreement or other basis for transmission that meets the requirements of the General Data Protection Regulation.

9. TO EMPLOYEES

9.1 It is forbidden to use the company's systems, or the equipment provided in contravention of the IT Policy. This includes the following non-exhaustive list:

a) Installation of unlawful or wilfully damaging applications

b) Download, upload or streaming of unlawful material

9.2 You can use your telephone and computer privately and commercially, provided that you do not disregard the principles of the IT Policy. This implies that your combined equipment must always be password protected. You should also be aware that your commercial use gives us the right to access information on your equipment while respecting your privacy.

9.3 You should pay close attention not to use your personal cloud services, e-mail accounts, or the like in connection with the processing of our Critical Data. It is strictly forbidden and may seriously harm us if your actions should cause a breach of security, such as leak of Personal Data.

9.4 The processing of our Critical Data may, to the extent necessary, include storage on portable media, such as USB keys, external hard disks, etc. If you make use of these, you must ensure the appropriate security, including encryption, password, physical locking, and subsequent destruction. You can ask the IT department for assistance.

9.5 If you discover, cause, or consider that there is a risk of a personal data breach, you must immediately stop ongoing activities (pull the plug) and inform the Chief Product Officer and the IT department immediately.

9.6 Any violation of the IT Policy provisions may have employment-related consequences. Gross violation will result in instant dismissal. It will be a mitigating circumstance if you report the violation.

10. CHANGES

10.1 The IT Policy shall be revised on a regular basis in case of changes in the situation of the company.