IT SECURITY POLICY

This Policy defines the security requirements implemented at Boyum IT for the proper and secure use of our IT services. Based on our IT Security Risk Analysis, our IT Security measures protect the organization and its users against security threats that could harm data security, data privacy, business integrity, and business reputation.

This Policy applies to all members of staff at Boyum IT and its subsidiaries, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access time to services. Any employees or freelancers who violate this policy can be subject to discipline, up to and including termination.

Any questions regarding internal systems, software, or hardware must be directed directly to it@boyum-it.com.

1. IT ASSETS POLICY

The IT Assets Policy defines requirements for the proper and secure handling of all IT assets at Boyum IT, incl. laptops, desktops, printers, and other equipment, applications, software, etc. for anyone using such assets, incl. internal users, temporary employees, visitors, and in general to any resources and capabilities involved in the provision of our IT services.

Losses, theft, damages, tampering, and other incidents related to assets that may compromise security must be reported immediately to the IT Department at it@boyum-it.com, cf. our Company Property Policy. More specifically:

1. **Working from home:**
   a. Rules for work performance apply irrespective of whether the work is done at home or in office locations, incl. rules on confidentiality and handling of confidential and/or sensitive information.
   b. The employee is responsible to ensure that any confidential information or Boyum IT resources he/she has access to are not accessible by anyone else. Rather than storing files on your personal computer, always save them on a Boyum OneDrive or network drive, which is easily accessible from home.
   c. In case your laptop or mobile device is corrupted by malware or a virus, your data can be restored.
   d. In case your laptop or mobile device is stolen, the data can easily be retrieved as we are not using disc encryption (bit locker). Please securely delete any files you copied to your local device.
   e. Do not let family members use your work computer.
2. **Computers provided by the company or purchased by the company:**
   a. Your company equipment will be delivered installed and configured by the IT Department.
   b. You cannot remove the equipment from the domain.
   c. You cannot reset/reinstall the operating system without written approval by the IT Department.
   d. You cannot remove any software provided by the IT Department.
3. **Installation of third-party software:**
   a. It is forbidden to install ANY third-party software without first getting written approval by the IT Department. There is a risk that harmful software gets installed without you knowing it.

4. Anti-virus software:

a. Anti-virus software is installed by the IT Department on all company-owned equipment. This CANNOT under any circumstances be removed. Doing so will be reported to your manager.

b. Anti-virus software must be installed and regularly updated on all privately-owned computers, incl. laptops if occasionally used for Boyum-related work. The anti-virus software will be provided by the IT Department. However, you must inform the IT Department at it@boyum-it.com that you installed company anti-virus software on a private computer, incl. the computer name.

c. Boyum IT anti-virus software must not be used on private computers that are not used for Boyum-related work.

2. ACCESS CONTROL POLICY

The Access Control Policy applies to all users in Boyum IT, incl. temporary users, visitors with temporary access to services, and partners with limited or unlimited time to services.

There is restricted access to all office facilities, either via the use of personal keys (at offices in Denmark, Belgium, Hungary, and the USA where access to the buildings is controlled by personal access keys) or normal keys (at offices in Spain and Germany).

All offices activate electronic alarms outside regular office hours.

Only key personnel has restricted access to infrastructure systems.

3. REMOTE ACCESS POLICY

Employees and freelancers with remote access privileges to Boyum IT's corporate network are responsible to ensure that their remote access connection is given the same consideration as the user's on-site connection to Boyum IT.

SAP Business One

You can access your own SAP Business One from outside a Boyum office through Remote Desktop (RDP) https://access.boyum-it.com. Log on with your credentials and domain password. Through the Remote Desktop, you can also access the internal file server.

You must be a member of an AD Group to access login through RDP or with VPN. The IT Department can assist with this.

MariProject and Internal file server

To access MariProject and the internal file server, you can use the VPN client (Pritunl). The IT Department will provide you with a VPN config file to be able to connect with the VPN. Laptops provided by IT will have this enabled by default.

If you connect to Boyum IT through VPN on a private computer, you are required to have a screen saver witha password enabled to prevent anyone from tampering with your computer or accessing Boyum IT network.

To protect our data, system, users, and customers, we follow and use the following precautions:

- Centralization of the installation and management and updating of anti-virus software on all systems using a cloud-based AV system with BitDefender.
- Updating of systems software (OS) regularly which is controlled by Windows Server UpdateServices (WSUS).
- Usage of administered firewall PFsense on all our locations.
- Usage of automatic screen lock on all our IT systems after 10 minutes of inactivity. Password must be entered to open the system again.
- Provision of remote access via encrypted Microsoft RDC and VPN.
- Implementation of network separation using IPSEC site-to-site VPN and VLAN separation to all remote offices.
    - Maintenance of back-ups on separate locations (remote backup location for important data).
    - Implementation of redundancy via virtual server environments (WMware cluster with failover).
- Storage of data in a data center which has access control with logging of access, cooling facility, and redundancy power supply incl. UPS.

4. PASSWORD CONTROL POLICY

A new employee will receive a temporary password from the IT Department. You need to have proper password controls in place, both in the office and when you're out and about. Put 'guest', 'password', '123456', and 'qwerty' in the bin. The first time you log in, you must change this password according to the following criteria.

A proper and secure Boyum IT password meets the following criteria:

- You cannot use any of your 24 last-used passwords.
- The maximum age of a password is 185 days.
- The minimum age of a password is 1 day.
- The minimum length of a password is 12 characters.
- A password cannot contain the user's account name or part of the user's full name exceeding two consecutivecharacters.
- A password contains characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Account lockout threshold = 5 invalid login attempts.

To remember your password, consider using a mnemonic device, for example, two-factor authentication where you have a password and a linked email or contact information for confirmation.

5. THE DATA PROCESSOR

The data processor will regularly conduct attention training concerning IT Security and the processing of personal data. The data processor will also implement segregation of duties concerning access control and rights management.

The data processor will evaluate the technical security on an ongoing basis to make upgrades if new technology can make the systems more secure at a cost which the data processor considers reasonable compared to the need for security.