boyum it

IT SECURITY POLICY

This policy defines the security requirements at Boyum IT for the proper and secure use of our IT services. These requirements are based on an IT Security Risk Analysis to protect the company from threats against the business and its operations, integrity, data privacy, and reputation. The IT Security Policy applies to all members of staff at Boyum IT Solutions and its subsidiaries, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access time to services.

Any questions regarding internal systems, software, or hardware, should go directly to it@boyum-it.com.

1. IT ASSETS POLICY

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

- Centralizing the installation, management, and updating of antivirus software on all systems using a cloud-based AV system.
- Updating systems software (OS) on a regular basis which is controlled by Windows Server Update Services (WSUS).
- Usage of administered firewalls in 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 RDP 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 (VMware cluster with failover).
- Storage of data in a data center that has access control with logging of access, cooling facility, and redundancy power supply including UPS.

2. IT ASSETS POLICY

The **IT Assets Policy** defines the proper handling of our IT assets (laptops, desktops, printers, applications, software, etc.). This applies to anyone using these assets (incl. internal users, temporary employees, visitors) and, in general, to any resources and capabilities involved in the provision of our IT services. More specifically:

1. **Computers provided or purchased by the company.**
    a. Your company equipment will be installed and configured by the IT department.
    b. You cannot remove the equipment from the domain.
    c. You cannot reset / re-install the operating system without agreeing on this with the IT department.
    d. You cannot remove any software provided by IT.

2. **Working from home**
    a. Rules for work performance apply irrespective of whether the work is done at home or in the office locations, incl. rules for confidentiality and handling of confidential and sensitive information.
    b. When working from home, the employee is responsible for ensuring that any confidential information or Boyum IT resources s/he 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 are easily accessible from home.
    c. In case your laptop or mobile device is corrupted by malware or virus, your data can be restored.
    d. In case your laptop or mobile device is stolen, the data can easily be retrieved (we do not use 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.

3. **Installation of third-party software**
    a. It is forbidden to install ANY third-party software that is not approved by IT. There is a risk that harmful software gets installed without you knowing it.

4. **Security breach**
    a. Losses, theft, damages, tampering, and other incidents related to assets that may compromise security must be reported immediately to the IT team at it@boyum-it.com.

5. **Anti-virus software**
    a. Anti-virus software is installed by IT 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 IT. However, you must inform it@boyum-it.com that you installed company anti-virus software on a private computer and inform the computer name.
    c. Boyum IT anti-virus software must not be used on private computers that are not used for Boyum-related work.

Please refer to our Company Property Policy for more details.

3. ACCESS CONTROL POLICY

The Access Control Policy applies to all users in Boyum IT Solutions, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access 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 have restricted access to infrastructure systems.

4. REMOTE ACCESS POLICY

Everyone with remote access privileges to Boyum IT's corporate network must ensure that their remote access connection is given the same consideration as an onsite connection to Boyum IT Solutions.

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 team 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 team will provide you with a VPN config file to be able to connect with 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 with password enabled to prevent anyone from tampering with your computer or accessing Boyum IT network. You are also required to have Boyum IT Antivirus software installed on the computer. Remember to notify the IT department that you have installed the Boyum IT Antivirus software on your personal computer.

boyum it

5. PASSWORD CONTROL POLICY

A new employee will receive a temporary password from the IT team. The first time you log in, you must change this password according to the following criteria. 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.

A good, Boyum IT secure password meets the following criteria:

- You can't use any of your 24 last used passwords.
- Maximum age of passwords is 185 days.
- Minimum age of passwords is 1 day.
- Minimum password length is 12 characters.
- Doesn't contain the user's account name or part of the user's full name exceeding two consecutive characters.
- 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 logon 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.

6. THE DATA PROCESSOR

- The data processor will on a regular basis conduct attention training in relation to IT security and the processing of personal data. The data processor will also implement segregation of duties in relation to access control and rights management.
- The data processor will evaluate the technical security on an ongoing basis with a view to making upgrades if new technology can make the systems more secure at a cost that the data processor considers reasonable compared to the need for security.