boyumit

IT SECURITY POLICY

This IT Security Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in Boyum IT. Its goal is to protect the organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

This document applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

1. IT ASSETS POLICY

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in Boyum IT. The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the IT Team immediately, cf. Company Property Policy.

When working from home, it is the responsibility of the employee to ensure that any confidential information or Boyum IT resources you have access to are not accessible by anyone else. Instead of storing Boyum IT files on your personal computer, save them always on a Boyum OneDrive or network drive, which are easily accessible from home. Securely delete any files you copied over. In case your laptop or mobile device is stolen or corrupted by malware or a virus, your data can be restored.

The general rules for work performance apply irrespective of whether the work is done at home or in the office locations, e.g. the rules on confidentiality and handling confidential and sensitive information. Anti-virus software must be installed and regularly updated on all privately-owned computers including laptops if occasional used for Boyum work when working from home. Don't let family members use your work computer. – don't connect our work devices to public hotspots.

2. ACCESS CONTROL POLICY

This policy applies to all the users in Boyum IT, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

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

Activating electronic alarms outside regular office hours

Only key personnel have restricted access to infrastructure systems

3. REMOTE ACCESS POLICY

It is the responsibility of Boyum IT employees and freelancers with remote access privileges to Boyum IT's corporate network 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 our 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 this desktop you can also access internal file server.

You need to be member of an AD group to access login through RDP. The IT team can assist with this.
You need to be member of an AD group to login 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 (currently we are using Pritunl). The IT team will provide you with a VPN config file to be able to connect with VPN. Any laptops provided by the IT team will have this enabled by default.

Antivirus software
Every computer used for Boyum IT work must be installed with antivirus software. Also, if you use your own private computer. Boyum IT will provide you with the software, but only on those computers that are connected to Boyum IT. The IT team can monitor, which computers are connected to Boyum IT servers. Laptops provided by the IT team are installed with antivirus software by default and MUST NOT be uninstalled.

If you use your private computer to connect to Boyum IT through VPN, we require to have a screen saver with password enabled, in order 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 these precautions:

- Centralizing the installation, management and updating of antivirus software on all systems using a cloud-based AV system with BitDefender
- Updating systems software (OS) on a regular basis – which is controlled by Windows Server Update Services (WSUS)
- Usage of administered firewalls 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 system again
- Provision of remote access via encrypted Microsoft RDC, & 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 which has access control with logging of access, cooling facility, redundancy power supply including UPS.

4. PASSWORD CONTROL POLICY

At the first day at Boyum IT, the IT team will assign you a temporary password. The first time you log in you can change this. You need to have proper password controls in place. This applies 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's:

- 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
- Do not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Contain 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

All those numbers and symbols can be tricky to remember, so try using a mnemonic device. Two-factor authentication is also a useful tool. That means having both a password and a linked email or contact information to confirm it's really you access your work material.

5. THE DATA PROCESSOR

- The data processor will on a regular basis conduct attention training in relation to IT security and processing of personal data. The data processor will also implement segregation of duties in relation to access control and rights management and new security measures is in the planning.

- The data processor will evaluate the technical security on an ongoing basis with a view 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.

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