Cyber Security Policy

Policy brief & purpose

Boardeaser's Cyber Security Policy outlines the company guidelines and provisions for preserving the data security and technology infrastructure.

The more a system rely on technology to collect, store and manage information, the more vulnerable it becomes to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation and overall business.

For this reason, we have implemented a number of security measures. We have also prepared instructions that will help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to Boardeaser's systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Undisclosed financial information
- Customer/partner/vendor data
- Patents, formulas and new technologies
- Customer lists (existing and leads)
- Information regarding IT-infrastructure

All employees are obliged to protect confidential data. Included in this policy are instructions for employees on how to avoid security breaches.

Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to accessed data. Boardeaser employees are instructed to keep both their personal and company issued computer, tablet and cell phone secure. Advised methodologies are:

- Keep all devices password protected
- Use and upgrade a complete antivirus software
- Never to leave devices exposed or unattended
- Install security updates of browsers and systems monthly or as soon as updates are available
- Log into company accounts and systems through secure and private networks only
- Use two-factor authentication whenever possible

Boardeaser also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

New hires are briefed on the above instructions to protect their devices, and to consult our Security Specialists if they have any questions.

When new hires receive company-issued equipment they will receive instructions for:

- Disk encryption setup
- Password management tool setup
- Installation of antivirus/anti-malware software
- Setting up two-factor authentication

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check and validate email addresses and names of people they receive a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they are instructed to consult our Security Specialists.

Manage passwords properly

Password leaks are dangerous since they can compromise an entire infrastructure. Not only should passwords be secure (as described below) to avoid being identified through guessing, they should also remain undisclosed.
For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to store their passwords, they are obliged to record it securely digitally and destroy the record when they no longer need to use the password.
- Exchange credentials only when absolutely necessary and with extreme care. When exchanging credentials in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change passwords every two months.
- Use two-factor authentication whenever and wherever possible.

Remembering a large number of passwords can be daunting. We encourage all of our employees to use a password management tool which generates and store passwords digitally and securely. Employees are obliged to create a secure password for the tool itself, following the above mentioned advise.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees are requested to consult our Security Specialists for assistance.
- Share confidential data over the company network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.

Our Security Specialists need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report suspected attacks,

suspicious emails or phishing attempts as soon as possible to our specialists. Our Security Specialists must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR/IT Department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Our Security Specialists should:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will use all physical and digital shields to protect information possible.

Remote employees

Remote employees must follow this policy’s instructions too. Since they will be accessing our company’s accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our Security Specialists/IT Administrators.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.