Cyber Security Policy

Version: 1.0.0

Effective date: 03/01/2020

Policy brief & purpose

Tispr cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

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

Scope

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

Policy elements

Confidential data

All employees are obliged to protect confidential data. In this policy, we will give our employees instructions 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 risks to our data. We advise our employees to keep both their personal and company-issued computers, tablets, and cell phones secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their 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.

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

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 emails and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, an excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can refer to Security Specialist

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. 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 write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them 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.
- We don't recommend using any software for password sharing such as LastPass, etc. New account creation should preferable to password sharing. When one account is shared between a few people it is hard to see who did any changes, etc
- Change their passwords every 90 days.
- Use two factors authentification in all services where it is available

Remembering a large number of passwords can be daunting. Employees may use the services of a password management tool that generates and stores passwords (1password, LastPass, KeyPassX, MacPass, etc). Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

Transfer data securely

Transferring data introduces a security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When the mass transfer of such data is needed, we request employees to ask our Security Specialist for help.
- 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 Specialist needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our Security Specialist must investigate promptly, resolve the issue and send a companywide alert when necessary.

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.

Accounts/Accesses Management to third party services

Everyone has to use only software from the company approved list (please contact your manager to check if the software is in the approved list until the list is not finalized). Please use google drive, confluence for documentation, and don't use Dropbox Paper or other 3rd party tools for documents

We will assign the owner for each of the 3rd-party services that we are using. This person will be responsible for account management and security from a usage perspective. The service Owner will be responsible for removing all accounts that are not used for more than 90days

Big amount of unused accounts in 3rd-party service increase data leaks probability. Employee must:

1. Inform Admin or Service Owner in case no needs accounts for this service anymore
2. Inform Admin or Service Owner in case no need for current permissions level
3. Inform Security Specialist if you have any concern that someone got access to your account in 3rd-party service

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 & Direct Manager*.
- 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.
- Use two-factor authentication in all services where it is available

Our Security Specialist should:

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

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 Specialist

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 trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity top of mind