MASTER WiZR

Company Cyber Security Policy

MASTER WiZR

Cyber Security Policy

Policy brief & purpose

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

This cyber security policy is for our employees, contractors, vendors, and partners to refer to when they need advice and guidelines related to cyber law and cyber crime. Having this cyber security policy we are trying to protect MASTER WiZR and its clients' data and technology infrastructure. This policy applies to all of MASTER WiZR employees, contractors, vendors, and anyone else who may have any type of access to MASTER WiZR systems, software, and hardware.

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

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this 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 risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone 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.

For new hires company gives instructions for:

- Disk encryption setup (when is needed);
- Password management tool setup;
- Installation of antivirus/ anti-malware software.

They should follow instructions to protect their devices and refer to our Security/IT team if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct our staff members 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 email 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, excessive number of exclamation marks.)

If a staff member isn't sure that an email they received is safe, they can refer to our IT Specialist.

Manage passwords properly

Password leaks are dangerous, 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 staff members 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 staff members needs 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, staff members should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

- Change their passwords every two months.

Staff members are obliged to create a secure password for the tool itself, following the abovementioned advice.

Transfer data securely

Transferring data introduces security risk. Staff members 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, we request staff members to ask our Security/IT team for help.
- Share confidential data over the company or other secure 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 IT team needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our staff members to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our IT team. Our IT team must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our IT team is responsible for advising staff members on how to detect scam emails. We encourage our staff members to reach out to them with any questions or concerns.

Additional measures

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

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to 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.

We also expect our employees to comply with our social media and internet usage policy.

Disciplinary Action

We expect all our staff members 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 contractor/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, contractors/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.