InfraGuard cyber security and data protection policy.

Cyber Security policy brief & purpose

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

We have implemented a number of security measures. We have also prepared instructions that may 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 our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists

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 services 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 do this by:

- 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.

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*

They will follow instructions to protect their devices and refer to our *Security Specialists/ Network Engineers* 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 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 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 an employee isn't sure that an email they received is safe, they can refer to our *IT 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.
- Change their passwords every two months.

- Use MFA for every authentication

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the above mentioned advice.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of any company data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our *IT Specialists/ Network Engineers* need 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 *IT Specialists/ Network Engineers* 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 the 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.

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

Our *Security Specialists/ Network Administrators* 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 these policies provisions as other employees do.

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

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 progessive 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.**Company data protection policy**

Data Protection Policy brief & purpose

InfraGuard's **Company Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Policy elements

InfraGuard, in the course of its operations, stores meta-data related to customer environments such as user names, patch install histories, pending patches, command logs and similar.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse

- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.