HERKIMER COUNTY INDUSTRIAL DEVELOPMENT AGENCY
CYBER SECURITY POLICY

Introduction:

This Cyber Security policy outlines the guidelines and gives a road map to preserve the security and data of The Herkimer County Industrial Development Agency (IDA). Because we rely on technology to collect, store, and manage information, we become more vulnerable to the severity of security breaches. Many of these breaches may be because of human errors, hacker attacks and system malfunctions. These situations can cause great financial burden and may jeopardize the reputation of the agency.

For this reason, there have been a number of security measures taken to avoid any risk. We have also prepared an instructional policy that may help mitigate the risk. This policy will highlight and explain the provisions.

Scope:

This policy applies to the office staff of the Herkimer Industrial Development Agency, and anyone who has access to the agency's software or hardware systems.

Policy Elements:

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Personal information (home addresses, social security numbers, etc.)
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. A timer will be set on all devices to automatically logout when not in use for a set period of time. This policy gives 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. Employees are to keep both personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.

- Do not leave devices exposed or unattended.

- Inform IT administration of pending security updates of browsers and systems monthly or as soon as updates are available.

- Ensure that all sensitive information is stored in a secured location that is subject to monitoring and backups, such as Goldmine, the S: drive, or the Herkimer IDA DropBox. Sensitive information should **not** be stored on local devices, such as a desktop or laptop hard drive.

- Log into company accounts and systems through secure and private networks only.

- Avoid accessing internal systems and accounts from other people's devices or lending your own devices to others.

Keep Emails Safe

Emails often host scams and malicious software (e.g. worms). To avoid virus infection or data theft, employees are 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 phrases or wording

- Check email and names of people you received a message from to ensure they are legitimate.

- Look for inconsistencies or giveaways (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 management staff or IT personnel.

Manage Passwords Properly

Password leaks are dangerous since they can compromise entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, employees are 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.

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 should ask IT administrator for help.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

Incident Response

Management and IT administration needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, employees are to report perceived attacks, suspicious emails or phishing attempts as soon as possible to management or IT. Management will contact the proper agency to investigate promptly, resolve the issue and send an agency-wide alert when necessary.

Management and IT administration 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 management.
- 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.

Management will work with IT administration to:

- 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.

Remote Employees

Remote employees must follow all company policies and regulations regarding cybersecurity and IT usage. 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.

Paper Disposal/Digital Disposal

In order to completely protect our information, we must ensure that in addition to being stored and transferred properly, it's also disposed of in a responsible manner. Any paper documentation containing the previously defined confidential data should be either stored in a secure location when not in use, or disposed of via cross-cut shredding. This shredding can be done via a shredder within the office or via a third-party document disposal service.

Any physical media containing confidential information digitally (hard drives of decommissioned computers, thumb drives no longer in use, CDs/DVDs, etc.) should be stored in a secured location or physically destroyed prior to disposal to ensure that any information contained within cannot be retrieved.

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: A verbal warning will be issued and further training the employee on security will take place.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): Will invoke more severe disciplinary action up to and including termination and/or legal action. 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.

Originally Adopted March 31, 2020
Re-adopted March 29,2022