CYBER SECURITY POLICY

Alliance's 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 business operations and reputation. For this reason, we have implemented numerous security measures and will continue to do so. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy. This policy applies to all associates, contractors, vendors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

This policy is to be used in conjunction with Alliance's policies regarding Acceptable Use of Company Equipment, Internet Use and the Bring Your Own Device to Work policy.

Identify

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- Unpublished financial information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)
- Associate information and data
- Proprietary information about projects or plans

All associates are obliged to protect this data at all times whether they are using it, viewing it or distributing it electronically or otherwise. If you have doubt about the confidential nature of a business document, assume it is confidential and discuss it with your supervisor. Do not disclose any company information without obtaining prior approval from you supervisor.

Protect

- Data storage

All company data and information must be saved and stored on the company's established SharePoint site. The SharePoint site is managed and controlled by the company's IT department. All access and approvals for access to relevant folders must be approved in advance by the Department head. Access will be audited on a regular basis and access will be immediately removed upon an associate's separation. Associates must not take or share information from the SharePoint to external parties unless they have received permission from their supervisors or unless the information does not contain confidential or proprietary information.

- Protect personal and company devices.

When associates use their digital devices to access company emails or accounts, they introduce security risk to our data. Associates must keep their personal and company-issued computer, tablet and cell phone secure. Any device, either company issued or personal, that is used to access company email or data must have the following protections:

- Every device must be password protected.
- Antivirus software must be installed.
- Do not leave the 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.

Associates must also avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.
All newly hired associates will receive company issued equipment with all required protections provided by IT. All new hires must also follow instructions and download all security software apps when putting company email or other company software on a personal device.

- Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, associates must:

- 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 the email address and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation points).

If an associate isn't sure that an email they received is safe, they must not click on anything in the email and instead forward it to ITSupport@allresco.com immediately. IT will investigate and block any and all suspicious emails and take any other appropriate action to eliminate the threat.

- 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. Therefore, when choosing passwords, Associates must adhere to the following guidelines:

- 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 associates need to write their passwords down, they are obliged to keep the paper or digital

document confidential, password protected and destroy it when their work is done.
- Do not exchange or share passwords.
- Change their passwords when prompted to by the Company standard regular prompt.

Alliance provides a self-service password management tool which generates and stores passwords. Associates are obliged to create a secure password for the tool itself, following the abovementioned advice.

➢ Transfer data securely

Transferring data introduces security risk. Associates must:
- Avoid transferring sensitive data (e.g. customer information, associate records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, associates must receive advanced approval from their supervisor and if needed, request help from IT at ITSupport@allresco.com.
- 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.

Detect & Respond

The IT department needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our associates to report perceived attacks, suspicious emails or phishing attempts as soon as possible to ITSupport@allresco.com. The IT department will investigate promptly, resolve the issue and send a companywide alert when necessary.
IT will train associates and regularly communicate with them on how to detect scam or suspicious emails. We encourage our associates to reach out to them with any questions or concerns.

➢ Additional measures

To reduce the likelihood of security breaches, associates must also take the following steps:
- Turn off their screens and lock their devices when leaving their desks – the IT controlled auto default to lock a company issued laptop is 15 minutes of non-use.
- Report stolen or damaged equipment as soon as possible to ITSupport@allresco.com.
- 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 associates to comply with our social media and internet usage policy.
To further reduce the risk of security breaches, the IT department will take the following actions and any others deemed appropriate (the below is not an exhaustive list):

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

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

- Remote associates

Remote associates must follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage any and all remote associates to seek advice from our IT department if they have any questions. Remote associates must also follow all of the rules and guidance outlined in the company's Remote Work Policy

- Disciplinary Action

We expect all of our associates to follow this policy at all times. If an associate's actions or failure to take action causes security breaches, the company may take disciplinary action up to and including termination. We will examine each incident on a case-by-case basis. Additionally, associates who are observed disregarding 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 associates and contractors, should feel that their data is safe. The only way to gain and keep 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.