MAP

RETIREMENT

MAP RETIREMENT CYBERSECURITY PROGRAM

INTRODUCTION

MAP RETIREMENT (MAP) believes that the company and each of its clients is a repository of non-public confidential information and that each respective party has an affirmative and continuing obligation to protect the security of the confidential information it maintains, as well as all confidential information it may access through its business relationships. The following MAP RETIREMENT Cybersecurity Program has been approved by senior leadership of MAP.

OVERVIEW OF INFORMATION SYSTEMS OPERATIONS

MAP RETIREMENT is headquartered in Appleton, Wisconsin. The network systems are managed and supported by MAP's IT department. Employees are issued a workstation and utilize Cloud technologies in leu of a physical server. MAP RETIREMENT has a variety of control mechanisms established, including password resets and dual authentication for logins. MAP uses anti-virus and anti-malware applications to protect systems from viruses and malicious code. Logical access to MAP's systems, applications, and data is limited to properly authorized MAP employees. MAP maintains backups that are stored off-site at a secure storage facility. MAP hosts an online application for client access called its Plan Access portal.

CYBERSECURITY AND DATA PRIVACY GOALS

The general procedures and safeguards MAP RETIREMENT has adopted to achieve its cybersecurity and confidentiality goals include, but are not limited to:

1. Ensure that MAP's infrastructure, information systems, and confidential information and data is protected from unauthorized access, use, or other malicious acts.
2. Identify and assess risks that may threaten MAP's assets, data, and systems on a periodic basis (no less than annually).
3. Protect against any anticipated threats or hazards to the security of MAP's assets, data, and systems.
4. Prepare for potential cybersecurity incidents by establishing an incident response plan and implementing detection, recovery, disclosure, and restoration procedures.

IDENTIFIED SECURITY AND CONFIDENTIALITY RISKS

MAP RETIREMENT recognizes that it is not possible to make a definitive list of all security and confidentiality risks to confidential information due to the rapidly changing and evolving technology landscape. However, MAP has recognized the following internal and external risks (this list is reviewed and assessed on a regular basis, no less than annually):

1. Unauthorized access to confidential information by an unauthorized individual.
2. Compromised computer system/network security as a result of system access by unauthorized personnel.

3. The physical or electronic interception or destruction of confidential information during transit.
4. Loss of confidential information and/or computer systems that contain confidential information due to a natural disaster.
5. Accidental or deliberate errors introduced into a computer system that contains confidential information.
6. Accidental or deliberate corruption of physical or electronic versions of confidential information.
7. Misuse of confidential information by MAP employees and/or representatives.
8. Requests for confidential information by unauthorized personnel.
9. Compromise of MAP's physical security that results in the unauthorized access of confidential information.
10. Unauthorized transfer of confidential information by or to a vendor.
11. Malware, viruses, or download of executable via e-mail or other file transfers to employees.

CYBERSECURITY INCIDENT RESPONSE

In the event of a cybersecurity incident, MAP RETIREMENT has established the following procedures to respond to the incident:

Notification of a possible cybersecurity incident.

1. MAP personnel will contact the MAP RETIREMENT IT department.
2. A business partner or outside source will contact MAP by means of whatever contact information they currently have. The MAP employee who receives the message will collect as many details as possible and forward this information to the MAP RETIREMENT IT department. Such information may include:
    a. The name of the caller.
    b. Time of the call.
    c. Contact information about the caller.
    d. The nature of the incident.
    e. The equipment and / or persons involved.
    f. Location of equipment or persons involved.
    g. How the incident was detected.
    h. When the event was first noticed that supported the idea that the incident occurred.

Contacted members of the MAP RETIREMENT IT department will evaluate the situation and determine a response strategy.

1. Is the incident real or perceived?
2. Is the incident still in progress?
3. What data or property is threatened and how critical is it?
4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?

5. What system or systems are targeted and where are they located both physically and on the network?
6. Is the incident inside the trusted network?
7. Is the response urgent?
8. Can the incident be quickly contained?
9. Will the response alert the attacker?
10. What type of incident is this? Example: virus, worm, intrusion, abuse, damage?

The MAP RETIREMENT IT department will notify the incident response team, which will be briefed on the cybersecurity incident. The incident response team will include, but not be limited to, the following MAP personnel: Managing Partners, CFO, IT, and Director of HR.

The incident response team members will establish and follow one of the following procedures, basing their response on the incident assessment:

1. Worm response
2. Virus response
3. System failure
4. Active intrusion response
5. Inactive intrusion response
6. System abuse
7. Property theft response
8. Website denial of service response
9. Database or file denial of service response
10. Malware response

The incident response team may implement additional procedures which are outside the scope of this plan. If there is no applicable procedure in place, the team may document what was done and establish a procedure for the incident.

Evidence Preservation – the incident response team will make copies of logs, emails, and other communication and will maintain a list of potential witnesses. The incident response team will also notify employees that information related to the incident must be preserved as long as necessary to complete prosecution and beyond in case of an appeal.

The incident response team will notify MAP RETIREMENT's cybersecurity insurance carrier of the incident and engage cybersecurity counsel to assist with evaluating the situation as appropriate.

Incident response team members will, internally or through external providers, use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel or providers should perform interviews or examine evidence, and the authorized personnel or providers may vary by situation.

Assess Damage and Cost – incident response team members will assess the damage to the organization and estimate both the damage cost and the cost of containment efforts.

Incident response team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

Incident response team members will restore the affected system(s) to the uninfected state. This may include, but is not limited to:

1. Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
2. Make users change passwords if passwords may have been compromised.
3. Ensure the system has been hardened by turning off or uninstalling unused services.
4. Ensure the system is fully patched.
5. Ensure real-time virus protection and intrusion detection is running.
6. Ensure the system is logging the correct events and to the proper level.

Documentation—the following shall be documented:

1. How the incident was discovered.
2. The category of the incident.
3. How the incident occurred, whether through email, firewall, etc.
4. Where the attack came from, such as IP addresses and other related information about the attacker.
5. What the response plan was.
6. What was done in response.
7. Whether the response was effective.

Notify clients whose employees' personal information may have been compromised. After the scope of the incident and the affected individuals have been determined, notification will occur without unreasonable delay unless a law enforcement agency has determined that notification will impede a criminal investigation. In such instances, client notification will occur as soon as the law enforcement agency determines that such notifications will not compromise its investigation. MAP may determine the language to be used in the notification, which may be distributed in either by a written notice, by e-mail, or by telephone (as permitted by law).

Notify proper external agencies—law enforcement and other appropriate agencies will be notified as recommend by legal counsel.

Review response and update policies—plan and take preventative steps so that a similar incident will not happen again.

1. Consider whether additional policy or policy adjustments could have prevented the incident.
2. Consider whether a procedure or policy was not followed which allowed the incident, and consider what could be changed to ensure that the procedure or policy is followed in the future.

3. Determine if the incident response was appropriate and evaluate whether it could be improved.
4. Determine if all appropriate parties were informed in a timely manner.
5. Consider whether sufficient changes have been made to prevent another occurrence.
6. Confirm that all systems have been patched and locked down, passwords changed, anti-virus updated, email policies set, etc.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

MAP RETIREMENT's Director of IT Operations will be primarily responsible for management of this Cybersecurity Program. The Director of IT Operations will meet periodically (no less than annually) to conduct a review of current security procedures and policies with MAP's cybersecurity team, which will include, but is not be limited to, the following MAP personnel: Managing Partners, CFO, Director of IT Operations, Director of Operations, and Director of HR. This will be done to help determine if security adjustments and or additional employee training are required. The team has the authority to respond, amend, or modify this program and is responsible for:

1. Assessing MAP RETIREMENT's risks associated with confidential information.
2. Preparing cost comparisons for varying confidentiality or security approaches appropriate to MAP's environment.
3. Creating standards that guide managers and employees in implementing MAP's security and confidentiality methods and procedures.
4. Making certain employees in the various work units, departments, and divisions in MAP abide by procedures and policies.
5. Maintaining comprehensive lists outlining:
    a) All confidential information repositories at MAP
    b) MAP hardware assets
    c) MAP software assets
    d) MAP telephone and facsimile connections.

In the event that exceptions and situations are not specifically outlined in its security policies and procedures, the President of MAP RETIREMENT will make the final decisions. The team relies on its Director of IT Operations to monitor applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements and to recommend technological changes to the system.

ACCESS CONTROLS AND IDENTITY MANAGEMENT

Administrative access controls have been established to restrict access to all MAP RETIREMENT systems and system resources that house confidential information. Access to MAP systems containing confidential information is provided only to those employees who need access to such system(s) to complete their assigned work. This section outlines various administrative controls including, but not limited to, access rights administration and authentication protocols as they pertain to computer networks, operating systems, and applications, via local and remote access. To help minimize the risk of unauthorized access, the following precautions have been instituted:

1. The access rights of each employee are configured at the proper level pertaining to the employee's position in the company (on a need-to-access basis).
2. Access privileges are reviewed on a recurring basis (no less often than every three months) and disabled or deleted as necessary.
3. All preconfigured "guest accounts" incorporated into hardware and software are disabled.
4. Mechanisms are in place to lock out users when there are repeated failed attempts to gain access.
5. All employees are made aware of the serious consequences that may result from security breaches and their individual responsibilities to help prevent incidences.

The Director of IT Operations is provided full system access to perform essential system administration functions critical to the continued operation of MAP RETIREMENT including, but not limited to: i) establishing User ID's; ii) maintaining authorization levels for all accounts; iii) terminating an employee's session; iv) correcting problems; v) removing users who no longer need access vi) and other broadly-defined system privileges. System administrator rights are restricted to only those employees whose job duties require them.

AUTHENTICATION PROCEDURES

Authentication involves the verification of a user's identity prior to providing access to computer resources. It is based on the user entering a unique username and password into the computer system to gain access to the system.

Upon request from a MAP RETIREMENT manager to grant initial system access, the Director of IT Operations will assign the employee to an existing access class. The employee is then given a registered and unique "User Name" that identifies the employee in the computer system and a password. The password must conform to established criteria to ensure the password is considered secure. The user is required to change his or her password no less often than every 90 days.

To mitigate Authentication related risks, MAP has adopted the following requirements:

1. Employee passwords are required to be a minimum of seven characters.
2. The password authentication system is protected by an encryption algorithm when a privileged user logs into the cloud remotely.
3. Lockout mechanisms are currently in place to lockout access to the User ID after five failed attempts.
4. All messages regarding failed log-ins are non-descriptive in nature.
5. If a workstation session is inactive for longer than fifteen minutes, a screen blanking mechanism is activated. Prior to resuming activity, the workstation user must re-enter their personal Windows PIN before any action can take place.

Multi-factor authentication, or similarly effective technology, will be used when feasible and appropriate. Specifically, when employees access cloud resources remotely, multi-factor authentication is required.

TECHNICAL SECURITY CONTROL PROCEDURES AND NETWORK SECURITY

To adequately secure access to MAP's systems and confidential information, a variety of control mechanisms have been established. The network controls that distinguish security domains include access control software permissions, firewalls, remote access servers, and Virtual Private Networks (VPNs). These network controls are kept up-to-date. To help identify and administer all of these access control points, a network diagram is continually updated to reflect any and all changes in the system's topology.

Information regarding the firewall is deemed sensitive and is included in MAP RETIREMENT's firewall standards. Those standards establish the rules for traffic coming into and going out of the MAP computer network and designate how the firewall will be managed. Areas covered by MAP's firewall standards include, but are not limited to:

1. Firewall topology and architecture
2. Types of firewalls being utilized
3. Monitoring firewall traffic when/if applicable
4. Permissible traffic
5. Firewall updating
6. Protocols and applications permitted based upon port filtering.

All administrative access to the DNS hosts, routers, and switches are limited to only a select number of system administrators and the Director of IT Operations. Remote administration must be done using encrypted communication and password authentication (including multi-factor authentication). To further secure any transmissions through the firewall, it has been configured to accept Network Address Translation and Virtual Private Network gateways.

Additional measures adopted by MAP to control access to the system software within the various SharePoint Sites include:

1. Restricted access to sensitive or critical Information.
2. Restricting user and program access to sensitive system resources including files, programs, or processes.
3. Regular updates to operating systems with security patches and using appropriate change control mechanisms.
4. Use of current and regularly updated antivirus software.
5. Use of network segregation, as appropriate.
6. System hardening, as appropriate
7. System backups are created outside of business hours on a daily basis. Each daily backup is retained for 12 months.

REMOTE ACCESS

All employees access MAP's cloud services remotely. SharePoint sites are managed by IT and access to data is controlled by employee level. For example, rank and file employees have no access to the financials of the company or our customers.

VULNERABILITY AND PATCH MANAGEMENT

MAP RETIREMENT's IT department is authorized and directed to conduct routine scans of systems, applications, and devices to identify vulnerabilities. Additionally, such scanning shall be part of each annual risk assessment conducted by MAP. A routine patching schedule will be established to deploy needed patches. Emergency patches will be made outside of the routine schedule based on the level of risk involved.

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

MAP RETIREMENT maintains a locked, access-controlled headquarters and satellite office. To mitigate external physical risks, such as fire, water, smoke, theft, destruction (accidental or by design), static electricity, dust and power surges, MAP has adopted various standards and procedures. Key elements of MAP's facilities security include, but are not limited to:

1. Access to MAP's office space is limited to one entrance.
2. The employee entrances are locked 24 hours a day with a code or key required for entrance.
3. The building is equipped with a variety of motion, fire, smoke, heat and glass break detectors. During non-business hours, an offsite security firm monitors the building security systems. Fire extinguishers with contents matched to the area of deployment have been placed throughout the building. They are inspected, serviced, and recharged by a licensed fire safety company.

ENCRYPTION

MAP uses encryption protocols a) when communications must be secured; b) for authentication processes; c) for the transmission of sensitive information; d) to secure applications and remote access communications.

ELECTRONIC AND PAPER-BASED MEDIA HANDLING

Confidential information is frequently contained on media such as paper documents, reports, backup tapes, optical storage, test data, and system documentation. The security of confidential information requires that such media be secured. MAP considers all media to be equally sensitive and therefore protects it all with equal diligence. Media handling and security is addressed in the following manner:

HANDLING AND STORAGE

All short-term storage of original media and media being worked on is kept on site at MAP until it is returned to the client, archived, or destroyed. All confidential information in long-term storage is packed, labeled, and arranged in a specific manner to reduce the risk of loss and destruction.

TRANSIT

MAP RETIREMENT is not responsible for the security of any confidential information a client physically transports to MAP until the confidential information is received by MAP. If confidential information is damaged or missing during transit, the applicable client is contacted.

DATA DISPOSAL

Paper-Based Confidential Information:
MAP RETIREMENT employees are prohibited from discarding any paper containing confidential information into regular trash bins. Pursuant to MAP's documented Shredding Guidelines, paper-based media with confidential information must be placed into locked and secured destruction bins that are emptied as they fill. Once a sufficient amount of paper-based media has accrued, a designated employee will make certain it is delivered to a designated media-disposal company. The media will then be destroyed in such a manner that it cannot be reasonably compromised or re-claimed.

Electronic-Based Confidential Information:
Since residual data frequently remains on electronic media even after erasure, all electronic-based media has specific disposal requirements. Electronic media is destroyed when it is no longer needed or used by MAP. Confirmation of destruction will be provided by MAP's electronic media destruction vendor.

SYSTEM, APPLICATION AND NETWORK SECURITY AND MONITORING

Logging and Data Collection

MAP takes steps to ensure sufficient data is collected to identify security incidents. MAP logs the following data:

1. Operating System Access
2. Remote Access

Malicious Code

MAP RETIREMENT defines malicious code as any program that acts in unexpected and potentially damaging ways. Since malicious code is highly dynamic, has many mobile connection possibilities, and does not specifically have to be targeted at MAP, it maintains a high-risk potential. To reduce risk and protect MAP systems from malicious code, MAP has established the following procedures including, but not limited to:

1. Use of anti-virus and anti-malware products, which use both signature and heuristic methods of detection and identification, on clients and servers.
2. Training system users not to open unexpected messages or executable files.
3. Training system users on what to do if they see an on-screen alert that a virus has been detected.
4. Use of email filters to prevent the receipt of executable files.

DATA GOVERNANCE AND CLASSIFICATION

MAP RETIREMENT seeks to ensure that its data is protected from unauthorized disclosure, access, alteration, or destruction, while preserving access to and use of data by authorized individuals. This policy is designed to provide guidance in determining the necessary safeguards that apply to each category of data. MAP classifies data/information as follows:

1. Restricted: Requires the highest level of security controls and only a specific group of employees are allowed access. Examples include MAP financial information and employee payroll, benefits, and HR data.
2. Confidential: Data which is restricted to necessary use to provide services to MAP's clients. Examples include client workforce census information, client lists, marketing plans, intellectual property, employee lists, and more.
3. Internal Use: Information designed for employee-only use and not for external distribution. Examples may include internal policies, procedures, forms, internal training materials, and employee guidelines and handbooks.
4. Public: Information with no sensitivity attached to it that likely will result in little or no risk if disclosed. Examples include public-facing forms, articles, and communications.

MAP's IT department will employ necessary controls to ensure that access to data is limited to properly authorized MAP employees. The access rights of each employee are configured at the proper level pertaining to the employee's position in the company (on a need-to-access basis). The access rights for each client are configured to limit access to the client's data. Client access can be further managed by the client to limit user access to specific types of data.

CONFIGURATION MANAGEMENT

MAP RETIREMENT has established controls regarding configuration management. Any configuration change must be reviewed for its security impact and its impact on end-users. Configuration change decisions, as well as the implementation details, are documented. Change Management Logs are available for review as part of any troubleshooting and incident response/management.

SYSTEMS AND APPLICATION DEVELOPMENT

MAP RETIREMENT understands that system and application development requires a consistent process for design and implementation. Software and applications must be adequately documented and tested before being used for business purposes and for storing data. MAP's IT department shall be responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC) to be employed in system and application development. At a minimum, the SDLC will take into account the following:

1. Definition and Project Initiation
2. Risk Assessment
3. Functional User Requirements
4. Technical and Architectural Systems Design
5. System Programming or Customized Off-the-Shelf Software Development
6. Quality Assurance
7. Documentation and Training
8. Systems Testing and Acceptance
9. Installation
10. Maintenance/Application Sunset

RISK ASSESSMENTS

On a regular basis, but no less frequently than annually, MAP conducts an annual risk assessment wherein threats are evaluated and categorized according to their potential risk level. The risk assessment will include an evaluation of how existing controls mitigate or address these threats. If needed, MAP's controls will be adjusted or revised to address changes in threats, systems, or business operations.

THIRD PARTY EVALUATION

On a regular basis, MAP shall engage a qualified third party to evaluate MAP's systems and produce a report of their findings. This report is expected to contain penetration test reports and supporting documents and analysis. Any corrections of vulnerabilities identified will be preserved along with the report.

CYBERSECURITY AWARENESS TRAINING

All MAP RETIREMENT employees are required to undergo extensive and ongoing cybersecurity training and testing. Such training and testing is conducted by internal and external resources. Initial training and testing occurs when an employee is first employed by MAP, and ongoing training and testing is required for all employees multiple times throughout the year. Topics covered in the cybersecurity training include, but are not limited to, phishing, spearphishing, social engineering, ransomware, passwords, safe web browsing, handling sensitive information, mobile device security, and CEO fraud.

VENDOR AND THIRD PARTY SERVICE PROVIDER MANAGEMENT

Should it be necessary to engage an outside vendor or third-party service provider, that vendor or third-party service provider will be subject to the following requirements:

1. The vendor or third-party service provider will be required to adhere to appropriate security controls that meet or exceed the standards set forth in this program.
2. The vendor or third-party service provider will be subject to initial and periodic risk assessments.
3. The vendor or third-party service provider must provide notice in the event of a cybersecurity incident impacting MAP's clients or data.
4. The vendor or third-party service provider will be required to have up-to-date access control policies and procedures (multi-factor authentication will be expected).
5. The vendor or third party service provider will be required to have up-to-date data encryption, access control (multi-factor authentication will be expected), and cybersecurity event notification policies and procedures.

ASSET INVENTORY AND MANAGEMENT

MAP RETIREMENT maintains an asset inventory list that documents all information assets, both hardware and software. This list is kept on MAP's Executive site on SharePoint. The inventory list is managed by MAP's IT Department who reviews the list and updates for additions or deletions. The asset inventory list shall be available for inspection by MAP's management at all times.

BUSINESS CONTINUITY / DISASTER RECOVERY PROGRAM

MAP RETIREMENT's Business Continuity / Disaster Recovery Plan addresses the risk mitigation and disaster recovery that would be necessary to protect MAP RETIREMENT and its clients in the event the plan must be implemented. Risk mitigation procedures have been assessed to cover a variety of contingencies including, but not limited to, the following:

1. Network, data systems, and cybersecurity incidents – MAP regularly works with its IT and operations teams to continually refine plans for disaster scenarios of varying severity and duration.
2. Natural disasters, acts of terrorism, pandemics, etc. – MAP works to continually assess and refine plans to respond to and mitigate the impact of a wide range of incidents.
3. Employee and client safety – MAP has developed plans to coordinate with appropriate law enforcement authorities and governmental agencies to prioritize the safety of MAP's employees and clients.
4. Training and communication – MAP's operations team, human resources, and others work to ensure that employees receive training and information necessary to implement MAP's Business Continuity / Disaster Recovery Plan. MAP has also established procedures for communicating to clients in the event that the Business Continuity / Disaster Recovery Plan has been implemented.

5. Alternate sites and communication methods – MAP has implemented procedures to ensure that MAP's mission critical systems, services, and operations can continue in the event of a disaster.
6. Business continuity / disaster recovery analysis and testing – MAP RETIREMENT periodically conducts workshops, exercises, and tests to assess response and recovery capabilities.

CONTINUING EVALUATION AND ADJUSTMENT

This MAP RETIREMENT Cybersecurity Program is subject to periodic review and adjustment. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the operations team and Director of IT Operations which will assign specific responsibility for MAP information technologies.

Addendum A

Employee Handbook Cyber Security Policy

208 Cyber Security

Policy brief & purpose

Our company 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.

For this reason, 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 financial information
- Data of customers/partners/vendors
- Patents, formulas, or new technologies
- Customer lists (existing and prospective)
- Advisor 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.
- Accept and install software upgrades when requested by MAP
- 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.

They should follow instructions to protect their devices and refer to our *Security Specialists/ Network Engineers* at Apollo Blue support@apolloblue.com 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 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 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.
• Never exchange credentials. If an exchange of credentials is required, please contact your supervisor and support@apolloblue.com.
• Change their passwords every two months.

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 necessary.
• All emails with any personal or confidential information regarding a client, participant, employee, advisor, accountant, census, plan specific information, company specific information be sent only in an encrypted format via email or uploaded through the secure client portal.
• The use of outside transfer programs is prohibited, examples include but are not limited to Box, Mantra, Dropbox, Google Drive, icloud.
• 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 [*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 your supervisor and our specialists. Our [*IT Specialists/ Network Engineers Apollo Blue-* ***support@apolloblue.com***] must investigate promptly, resolve the issue, and send a companywide alert when necessary.

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/ 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.

Our [*Security Specialists/ Network Administrators*] 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 this 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 a large-scale breach (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 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.