Information Technology Policy and Procedure

alpha bold
5857 Owens Avenue, Suite 2148,
Carlsbad, CA 92008
(909) 979-1425

Table of Contents

Introduction

The AlphaBOLD IT Policy and Procedure Manual provides the policies and procedures for selection and use of Information Technology within the business which must be followed by all staff. It also provides guidelines AlphaBOLD will use to administer these policies, with the correct procedure to follow.
Information technologies includes, without limitation, computers, computer-based networks, computer peripherals, operating systems, e-mail, Intranet, software or any combination thereof, that are made available by AlphaBOLD for supporting its goals of providing quality products and services to customers, increase shareholder value and foster employment satisfaction.
AlphaBOLD will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.
To preserve the integrity of the information technology systems against accidents, failures or improper use, AlphaBOLD reserves the right to limit, restrict or terminate any user's access and to inspect, copy, remove or otherwise alter any data, file or system resources.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.
These policies and procedures apply to all employees.

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of AlphaBOLD's resources. All users, including contractors, clients and vendors with access to AlphaBOLD's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any AlphaBOLD's facility, has access to the AlphaBOLD's network, or stores any non-public AlphaBOLD's information.

4.0 Policy

4.1 General

1. All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least a quarterly basis.
3. Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
4. All user-level and system-level passwords must conform to the guidelines described below.

5.0 Password Protection

1. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
2. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
3. Always use different passwords for AlphaBOLD accounts from other non-AlphaBOLD access ID's (e.g., personal ISP account, option trading, benefits, etc.)

If an account or password compromise is suspected, report the incident to the Information Security Department.

6.0 Password Requirements

1. Minimum Length - 8 characters recommended
2. Maximum Length - 14 characters
3. Minimum complexity -. Passwords should use following three types of characters:
    1. Lowercase
    2. Uppercase
    3. Numbers
4. Passwords are case sensitive, and the user name or login ID is not case sensitive.
5. Password history - 3 Passwords
6. Maximum password age 0 days
7. Minimum password age 0 days
8. Account lockout threshold – 3 failed login attempts

7.0 Application Development Standard

Application developers must ensure their programs contain the following security precautions.

Applications:

1. Shall support authentication of individual users, not groups.
2. Shall not store passwords in clear text or in any easily reversible form.
3. Shall provide for some sort of role management, such that one user can take over the functions of Another without having to know the other's password.
4. Shall support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval wherever Possible.

8.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random

basis by the Information Security Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Remote Access Policy

1.0 Overview

This remote access policy specifies how remote users can connect to the main organizational network and the requirements for each of their systems before they can connect. This will specify:

2.0 Purpose

The purpose of this policy is to define standards for connecting to AlphaBOLD's network or any client's networks. These standards are designed to minimize the potential exposure to AlphaBOLD from damages which may result from unauthorized use of AlphaBOLD resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical AlphaBOLD internal systems, etc.

3.0 Scope

This policy applies to all AlphaBOLD employees, contractors, vendors and agents with an AlphaBOLD-owned or personally-owned computer or workstation used to connect to the AlphaBOLD, or AlphaBOLD's Clients Networks. This policy applies to remote access connections used to do work on behalf of AlphaBOLD, including reading or sending email and viewing intranet web resources.

4.0 Approval

Any remote access using either dial-in, VPN, or any other remote access to the organizational network must be reviewed and approved by the appropriate supervisor. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

5.0 Remote Computer Requirements

1. The anti-virus product called Windows Defender Antivirus is always required to be operating on the computer in real time protection mode.
    1. The product shall be configured for real time protection.
    2. The anti-virus library definitions shall be updated at least once per week.
    3. Anti-virus scans shall be done a minimum of once per week.

The computer must be protected by a firewall at all times when it is connected to the internet.

5.1 VPN Requirements

1. Client Check - A requirement that must be set for VPN clients is that a firewall must be installed and operational. Also, Anti-virus software must be installed and operational. If the VPN client does not meet the criteria, either the connection is not allowed, or the client can only access a limited area where they can get the software needed to meet the requirement.
2. The connection choices are PPTP, L2TP, IPsec, and Authentication -

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Internet Connection Policy

1.0 Overview

This internet connection policy requires users to use the internet for business only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent.

2.0 Purpose

This policy is designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

All physical internet connections or connections to other private networks shall be authorized and approved by

3.0 Use of the Internet

1. All employee use of the internet shall be for business purposes only.
2. Employee use of the internet may be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.

Employees are urged to use caution when visiting unknown internet sites and through user training set and keep their browser configured to IT approved standards to protect against infections of malware.

4.0 Internet Control and Logging System

The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.

1. The ability to log user internet activity including:
    1. Time of the internet activity.
    2. Duration of the activity.
    3. The website visited.
    4. Data and type of data downloaded
2. The system (will | will not) require a login ID or it will use the current network login to identify users.

The system used to prevent users from visiting inappropriate, pornographic, or dangerous web sites shall be Net screen. Duration of the activity, the website visited, and any data downloaded, and the type of data downloaded. The system will cache web pages.

5.0 Enforcement

Since improper use of internet can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

Asset Control Policy

1.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them, but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets. .

2.0 Purpose

This policy is designed to protect the organizational resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

3.0 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

3.1 IT Asset Types

This section categorized the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Printers, Copiers, FAX machines, multifunction machines
4. Handheld devices
5. Scanners
6. Servers
7. Firewalls
8. Routers
9. Switches
10. Memory devices

3.2 Assets Tracked

. Assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data.
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

4.0 Asset Tracking Requirements

1. All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired, or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

6.0 Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.
4. Asset disposal

In all these cases the asset transfer checklist must be completed.

7.0 Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed prior to disposal. Any data storage devices. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special techniques. Approved technologies are to specify in a Media Data Removal Procedure document by asset type including:
    1. Memory stick
    2. CD ROM disk
    3. Storage tape
    4. Hard drive.
    5. RAM memory
    6. ROM memory or ROM memory devices.

8.0 Loss, Theft or Damage to assets

A loss, theft or damage to the Organization's assets may be the result of accidental loss or damage, or unavoidable theft or robbery. Alternatively, it may be due to circumstances within a person's control, such as simple negligence, gross negligence or willful misconduct on the part of individuals or groups of individuals.

- **Simple negligence** is a failure to act as a reasonably prudent person would have acted under the same or similar circumstances.
- **Gross negligence** is a failure to exercise even a slight degree of care, or an extreme departure from the course of action expected of a reasonable person, all circumstances considered.
- **Willful misconduct** is an intentional or deliberate violation of rules or policies, including fraud and dishonesty.

9.0 Essential procedures

1. AlphaBOLD personnel have an individual responsibility to prevent losses and promptly notify the IT and Operation Teams when a theft or loss occurs for review.
2. Appropriate legal actions should be taken when a theft or loss occurs.
3. IT, Operations team will review the incident and determine the applicable value of the missing property and also will ascertain the circumstances surrounding the theft, loss, damage or destruction of the Organization's property and will submit its findings and conclusions to the Director of Operations and Finance.
4. Director Operations and Finance will then notify the person concerned whether he or she will be held financially responsible
5. for the damage, loss or theft of the Organization's property or is absolved from responsibility.

10.0 Financial responsibility

AlphaBOLD personnel may be held personally responsible for loss or damage caused through negligence or misconduct. The level of responsibility and reimbursement will depend on whether the loss or damage

was due to simple negligence, gross negligence or willful misconduct and whether there are extenuating or mitigating factors.

- When an asset or piece of equipment has been damaged due to simple negligence, the amount of reimbursement will be the total cost of repair or the fair market value of the asset or equipment, whichever is lower.
- When an asset or piece of equipment has been damaged due to gross negligence or willful misconduct, the amount of reimbursement will be the total cost of repair or the current replacement cost of the asset or equipment.

Mobile Computer Policy

1.0 Overview

This policy defines the use of mobile computers in the organization. It defines:

1. The process that mobile computers must meet to leave the corporate network. Both the device and any sensitive data should be password protected.
2. How mobile computers and devices will be protected while outside the organizational network.
3. The process that mobile computers must meet to enter the corporate network when being brought into a building owned by the organization.

2.0 Purpose

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

3.0 Scope

This policy covers any computing devices brought into the organization or connected to the organizational network using any connection method. This includes but is not limited to desktop computers, laptops, and palm pilots.

Note:

To write this policy, consider data and the sensitivity of the data stored and viewed on the mobile computer including:

1. Email
2. Data the user is working on that is stored locally.
3. Data from the internal network that the user may access while the computer is outside the network.
4. Locally stored user names and passwords.

Consider loss due to:

5. Theft - should locally store data be encrypted?
6. Hard drive failure

4.0 Responsibility

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile computer and agrees to adhere to this policy. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator. The user of the computer agrees not to use the mobile computer for personal business and agrees to abide by the organizational computer usage policy.

5.0 Connection Terms

7. Devices connected to the organizational network must be determined to be a benefit to the organization rather than convenience by the designated IT manager.
8. All mobile devices owned by the organization or allowed on the organization network must be identified by their MAC address to the IT department before being connected. (Possibly require static IP address)
9. The device must meet the computer connection standards described in the following section.
10. The device operator must be identified by name and contact information to the IT department.
11. The computer device operator must be familiar with the organization's acceptable use policy.
12. Devices not owned by the organization are subject to a software audit to be sure no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.
13. Access rights to the organizational network cannot be transferred to another person even if that person is using an allowed computing device.

6.0 Mobile Computer Protection

1. Any mobile computer owned by the organization shall always operate the following for its own protection:
    1. Antivirus program named Windows Defender Antivirus with the latest possible virus updates. The program shall be configured for real time protection, to retrieve updates daily, and to perform an anti-virus or malware scan at least once per week.
    2. A firewall program named _Windows firewall with the latest possible updated. The program shall be operational any time the computer is connected to any untrusted network including the internet to protect the computer from worms and other malware.
    3. Additional malware protection software shall be active on the computer in accordance with the anti-virus and malware policy.
    4. The operating system and application patch levels must be consistent with the current patch levels of our organization for similar devices and operating systems.
2. Policy for mobile computers owned by the organization and removed nightly by employees with permission to work from home.
    1. These computers shall always meet requirement 6.0.1 above.
    2. It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password. Operating systems that do not safely support this

process shall not be used in mobile computers. The IT Security department will determine and specify the proper tools to be used for authentication and access controls.

3. The computer shall be checked monthly by IT Security department personnel at designated times when the computer will be entering a secure building area. The check will include a scan for malware and a test to determine whether the computer has a worm. The state of stored sensitive data shall also be checked to determine whether it is encrypted and whether data of too high a level of security is being stored on the computer. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.

7.0 Protecting the Network

Mobile computers entering the network shall meet the following requirements.

1. If the computer is owned by the organization and used regularly by employees according to 4.0 above, then the computer shall be checked according to that part of the policy.
2. If the computer is owned by the organization and is returning from a period when an employee used it for travel, the following check shall be performed.
    1. Determine whether the anti-virus program is up to date, has the latest virus definitions, is configured properly, and is running properly. If it fails one of these conditions or has not been scanned for a virus within the last week, a full virus scan must be done before the computer can be used in the building.
    2. Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
    3. Test the state of stored sensitive data to be sure it is encrypted.
    4. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.

8.0 Enforcement

Since improper use of mobile computers can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

Bring Your Own Device (BYOD) Policy

1.0 Overview

AlphaBOLD recognizes the benefits that can be achieved by allowing its employees to use their own electronic devices. Such devices include laptops, smart phones and tablets, and the practice is commonly known as ‘bring your own device’ or BYOD.

2.0 Purpose

This Policy is required to ensure that AlphaBOLD remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.
It is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing AlphaBOLD provided services on BYOD

3.0 Acceptable Use

1.0 The company defines acceptable business use as activities that directly or indirectly support the business of AlphaBOLD.
2.0 The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
3.0 Devices may not be used at any time to:
- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in outside business activities
- Etc.

4.0 AlphaBOLD has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

5.0 Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

6.0 Security

- To prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's password policy should be followed.
- The device must lock itself with a password or PIN if it's idle for two minutes. After five failed login attempts, the device will lock. Contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.

- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

7.0 Risks/Liabilities/Disclaimers

- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours.
- Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is always expected to use his or her devices in an ethical manner and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- AlphaBOLD reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

System Update Policy

1.0 Overview

This policy is an internal IT policy which defines how often computer system updates are done and under what conditions they are done.

2.0 Purpose

This policy is required to establish a minimum process for protecting the organizational computers on the network from security vulnerabilities. This policy shall determine how updates are done for both servers and workstations, and who is responsible for performing the updates along with specifying the tools used to perform system updates.

3.0 Update Requirement Determination

This section defines methods used to determine what updates should be done and when they should be applied.

3.1 Update Types

Several types of updates may be required on any computer and all the types should be considered for the below listed computer system components. They include:

1. The operating system.

2. Application updates.

3.2 Update Checking

There are several methods to determine when updates should be performed.

1. Review of posted security flaws and patches for each type of update applicable to the computer system.
2. An automatic scanning of the system to determine available updates not yet applied to the system or application.

The review of posted security flaws and patches should always be used for the computer operating system, BIOS, and applications. The manufacturer website should be used and there may also be other appropriate sites posting relevant bulletins. If an automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate

4.0 Server Updates

Server updates shall be done by a qualified and authorized system administrator. Updates for servers shall be checked no less than monthly to determine whether any new updates to any computer system components are required. The system administrator shall determine the following:

1. Whether the update applies to the computer system under consideration.
2. Whether the update is safe to apply or whether it make break an application or some other part of the operating system where functionality is required.

A test environment should be used to determine whether updates may break functionality prior to implementation of production environments. The ability to provide a test environment and thoroughness of determining whether any functionality is broken by the update will vary from organization to organization depending on available resources.

5.0 Workstation Updates

Workstation updates may be done using any provided tools depending on the type of workstations and their operating systems. In this policy workstation updates shall be performed using Microsoft Windows update Tool.

Incident Response Plan

1.0 Overview

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handling various security incidents. This document discusses the considerations required to build an incident response plan.

2.0 Designated Person

Ahmad Bilal IT/DevOps Lead is responsible of all compliance and Data Protection related tasks and issues.

In case of any incident

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion.

3.0 Incident Response Goals

1. Verify that an incident occurred.
2. Maintain or Restore Business Continuity.
3. Reduce the incident impact.
4. Determine how the attack was done or the incident happened.
5. Prevent future attacks or incidents.
6. Improve security and incident response.
7. Prosecute illegal activity.
8. Keep management informed of the situation and response.

4.0 Incident Definition

An incident is any one or more of the following:

1. Loss of information confidentiality (data theft)
2. Compromise of information integrity (damage to data or unauthorized modification).
3. Theft of physical IT asset including computers, storage devices, printers, etc.
4. Damage to physical IT assets including computers, storage devices, printers, etc.
5. Denial of service.
6. Misuse of services, information, or assets.
7. Infection of systems by unauthorized or hostile software.
8. An attempt at unauthorized access.
9. Unauthorized changes to organizational hardware, software, or configuration.
10. Reports of unusual system behavior.
11. Responses to intrusion detection alarms.

5.0 Incident planning

In the incident response plan, do the following:

1. Define roles and responsibilities
2. Establish procedures detailing actions taken during the incident.
    1. Detail actions based on type of incident such as a virus, hacker intrusion, data theft, system destruction.
    2. Procedures should consider how critical the threatened system or data is.
    3. Consider whether the incident is ongoing or done.

6.0 Incident Response Life cycle

1. Incident Preparation
    1. Policies and Procedures

        1. Computer Security Policies - These involve many policies including password policies, intrusion detection, computer property control, data assessment, and others.
        2. Incident Response Procedures
        3. Backup and Recovery Procedures
    2. Implement policies with security tools including firewalls, intrusion detection systems, and other required items.
    3. Post warning banners against unauthorized use at system points of access.
    4. Establish Response Guidelines by considering and discussing possible scenarios.
    5. Train users about computer security and train IT staff in handling security situations and recognizing intrusions.
    6. Establish Contacts - Incident response team member contact information should be readily available. An emergency contact procedure should be established. There should be one contact list with names listed by contact priority.
    7. Test the process.
2. Discovery - Someone discovers something not right or suspicious. This may be from any of several sources:
    1. Helpdesk
    2. Intrusion detection system
    3. A system administrator
    4. A firewall administrator
    5. A business partner
    6. A monitoring team
    7. A manager
    8. The security department or a security person.
    9. An outside source.
3. Notification - The emergency contact procedure is used to contact the incident response team.
4. Analysis and Assessment - Many factors will determine the proper response including:
    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, where are they located physically and on the network?
    6. Is the incident inside the trusted network?
5. Response Strategy - Determine a response strategy.
    1. Is the response urgent?
    2. Can the incident be quickly contained?
    3. Will the response alert the attacker and do we care?
6. Containment - Take action to prevent further intrusion or damage and remove the cause of the problem. May need to:
    1. Disconnect the affected system(s)
    2. Change passwords.
    3. Block some ports or connections from some IP addresses.
7. Prevention of re-infection
    1. Determine how the intrusion happened - Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, attack due to unpatched system or application.

2. Take steps to prevent an immediate re-infection which may include one or more of:
    1. Close a port on a firewall
    2. Patch the affected system
    3. Shut down the infected system until it can be re-installed
    4. Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
    5. Change email settings to prevent a file attachment type from being allow through the email system.
    6. Plan for some user training.
    7. Disable unused services on the affected system.
8. Restore Affected Systems - Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following
    1. Re-install the affected system(s) from scratch and restore data from backups if necessory. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
    2. Make users change passwords if passwords may have been sniffed.
    3. Be sure the system has been hardened by turning off or uninstalling unused services.
    4. Be sure the system is fully patched.
    5. Be sure real time virus protection and intrusion detection is running.
    6. Be sure the system is logging the correct items
9. Documentation - Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.
10. Evidence Preservation - Make copies of logs, email, and other documentable communication. Keep lists of witnesses.
11. Notifying proper external agencies - Notify the police if prosecution of the intruder is possible.
12. Assess damage and cost - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
13. Review response and update policies - Plan and take preventative steps so the intrusion can't happen again.
    1. Consider whether an additional policy could have prevented the intrusion.
    2. Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
    3. Was the incident response appropriate? How could it be improved?
    4. Was every appropriate party informed in a timely manner?
    5. Were the incident response procedures detailed and cover the entire situation? How can they be improved?
    6. Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    7. Have changes been made to prevent a new and similar infection?
    8. Should any security policies be updated?
    9. What lessons have been learned from this experience?

Cloud Resources Security Policy

1.0 Overview

AlphaBOLD has no on-prem footprints and heavily relies Cloud Services for all its infrastructure, applications, and development environments to meet the organization requirements. This policy draws an outline on provisioning, managing, and securing the cloud infrastructure and applications to ensure the data security and privacy requirements.

2.0 Purpose

This policy outlines best practices and approval processes in relation to the use of cloud computing solutions. This Policy is required to ensure that AlphaBOLD remains in control of the data for which it is responsible, regard. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

3.0 Scope

This policy applies to the all cloud services being used or in consideration to host any application or services to meet the business requirements, which includes but not limited to Azure IaaS, PaaS, SaaS Services office 365 and Microsoft 365 services, Freshdesk Ticketing system, GoDaddy and any other cloud services from any vendor.
This policy also applies to all AlphaBOLD individuals that have been granted access to any cloud resources and required to have strict compliance of this policy.

4.0 Policies

Azure Cloud resources Security Policy

Azure IaaS

- Azure compute resources should be protected with two level firewalls and network security groups.
- Wildcard access should be strictly restricted
- All firewall related changes should be managed through IT Support Team
- Access should be allowed from trusted IP addresses
- No user should be having owner access to any Azure resources except IT
- All VM's should be configured to use Azure AD authentication and for local account Password should be complaint with the AlphaBOLD's Password Policy.
- All web servers hosted in Azure should be SSL protected with strong cypher/encryption techniques.
- All VM's OS level Updates should be regular installed
- Windows Defender should be enabled and regularly updated
- Use a least privilege approach when granting access to the VM's.

- Enable disk level encryption
- Always use Azure Key Vault to store and secure Passwords and Secrets.

Azure PaaS

- SQL Authentication should be blocked and use Azure AD authentication for all SQL connections.
- Azure Database Server should be firewall protected and only whitelisted IP address should be allowed to access the databases
- Shared access signatures (SAS) should be used.
- Role-based access control (RBAC) should be implemented
- Client-side encryption for high value data should be enabled
- Storage Service Encryption should be used.
- Storage accounts should not have any public access.
- Azure App services should be authenticated through Azure AD
- RBAC should be applied and only required resources should have access to the app services
- Security Keys should be protected
- Incoming source IP's should be restricted wherever possible.

GoDaddy

- Quarterly Security and Access reviews should be performed on all Hosting accounts.
- Access review reports should be saved on IT/DevOps SharePoint Document library
- Restrict access to WordPress admin to IT support team only
- Ensure all passwords are following AlphaBOLD Password policy
- Regularly review all install plugin and update if required.
- Unnecessary plugins should be removed from all Production sites
- Website security and malware protection should be enabled for all production sites

Office 365

- Quarterly Security and Access reviews should be performed for Admin accounts, SharePoint online and Dynamics CRM Production environment.
- Quarterly perform attack simulations using Microsoft Attach simulator and submit the report to all stakeholders.
- Multifactor Authentication should be enabled for all accounts including service accounts, guest accounts and app service accounts.
- SPF and DKIM should be enabled for all mail enabled domains.
- Auditing and logging should be enforced for all users.
- MDM Device compliance checks should be reviewed biweekly and ensure all Company owned devices should be compliant with the MDM polices.
- Use Role based access controls.
- Right management configuration should be review on quarterly basis and reports should be shared with all stockholders.
- Implement Office 365 Information Protection for GDPR using Microsoft Security and ensure AlphaBOLD's security posture meets the GDPR requirements.

5.0 Compliance

Implementation of this Policy will be subject to periodic review by Internal IT Audit Team,

as appropriate, as part of AlphaBOLD's risk management framework.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.