afiniti

MAKING CHANGE STICK

Title

Information Security Policy V4

Date

July 2018

Review date

June 2019

INSPIRE > INVOLVE > INTERACT

0845 608 0104 - info@afiniti.co.uk - www.afiniti.co.uk

TOP 20 LEARNING PROVIDER 2018

Learning & Performance Institute
Accredited Learning Provider
Gold Standard

Institute of Internal Communication
The power within

Corporate Member
Change Management Institute

Contents

Information Security 3
1 Information Security Policy 4
1.1 Introduction 4
1.2 Purpose 4
1.3 Scope 4
1.4 Responsibilities 4
1.5 Related Documents 5
1.6 Principles 5
2 Policy elements 6
2.1 Classification of Information 6
2.2 Recruitment 7
2.3 Asset Management 7
2.4 Physical Security 8
2.5 System & Data Backups 8
2.6 Malware 9
2.7 Internet Access 9
2.8 External Network Access 10
2.9 Systems Access, User IDs and Passwords 10
2.9.1 Systems Access 10
2.9.2 User IDs 11
2.9.3 Passwords 11
2.9.4 Unattended Equipment 11
2.10 Mobile Computing 12
2.11 Systems Design 12
2.12 Testing 12
2.13 Change Management 13
2.14 Business Continuity 13
2.15 Legal Requirements 14
3 Version History 15

Information Security

Information is an asset which, like other important business assets, has value and needs to be suitably protected. *Information Security* is defined as the preservation of information confidentiality, integrity and availability.

- *Confidentiality:* ensuring that information is accessible only to those authorised to have access.
- *Integrity:* safeguarding the accuracy and completeness of information and processing methods.
- *Availability:* ensuring that authorised users have access to information and associated assets when required.

1 Information Security Policy

1.1 Introduction

This Information Security Policy is approved and authorised by Afiniti Directors and Senior Management.

Failure to comply with the Policy, either deliberately or through negligence could result in disciplinary action.

It is the responsibility of Afiniti leadership to ensure that publications on the Information Security Policy are made available to their staff and contractors.

Afiniti personnel refers to staff, partners and associates. All of whom will sign a statement agreeing to abide by the terms of this Information Security Policy and any specific client requirements.

1.2 Purpose

The purpose of the Information Security Policy is to define the requirements for the protection of the Afiniti and its clients' information assets from all threats, whether deliberate or accidental, with the objective of ensuring business continuity and minimising the impact of security breaches.

1.3 Scope

The IT Security Policy applies to:

- All Afiniti data and information regardless of processing mode (e.g. manual or computer) and storage mode (including but not limited to electronic, hard copy form, etc).
- All client data and information regardless of processing mode (e.g. manual or computer) and storage mode (including but not limited to electronic, hard copy form, etc).
- All data processing activities performed within or on behalf of Afiniti (including but not limited to all divisions, subsidiaries, affiliates, joint ventures, etc).
- All personnel contracted to undertake work for Afiniti (including but not limited to permanent employees, partners, associates etc).

1.4 Responsibilities

The following states specific responsibilities for Afiniti's Information Security Policy.

- Definition, publication, updating and dissemination of Afiniti's Information Security Policy is the responsibility of Afiniti Leadership.
- Afiniti Leadership are responsible for providing Afiniti personnel with secure systems which meet their business needs.
- Where the Associate decides to use their own devices(s) to fulfil their obligations to Afiniti and its clients then they are responsible for compliance to this policy and all that it entails.
- Implementation of Afiniti's Information Security Policy is the responsibility of Afiniti Leadership departmental leaders.

- Leadership are responsible for ensuring that Afiniti personnel are fully aware of the requirements of the Information Security Policy and its associated standards.
- Leadership are also responsible for the security of information that is being processed in the area under their control.
- It is the responsibility of all Afiniti personnel to read, understand and comply with the appropriate aspects of this policy and any accompanying procedures.

1.5 Related Documents

- Data Protection Policy
- Privacy Policy
- Business Recovery & Cyber Response Plan
- Data Breach procedure

1.6 Principles

The following are the key principles behind Afiniti's Information Security Policy.

- **Afiniti personnel will comply with all regulatory and legislative requirements** – to maintain our position as a reputable and responsible organisation.
- We will **adhere** to the compliance requirements of our **clients.**
- **Risks will be assessed and action taken accordingly -** to ensure we maintain a balance between the cost of security and the value of the information we are protecting.
- **Access to information will be controlled** – to protect our clients and business partners, and our specialist knowledge and business interests.
- **Corporate information resources will be used only for permitted purposes** – to ensure the right resources are available, as and when required, to support the business.
- **Business continuity and contingency plans will be developed and periodically tested** – to ensure we are able to continue with critical business functions in the event of a major incident or disaster.
- **Personnel will be given appropriate information security awareness training** – to ensure they have the skills, knowledge and ability to comply with policies defined to protect our information.
- **Individuals will be accountable for their actions with respect to information resources** – to ensure that perpetrators of illegal, unethical, unsociable, or incompetent behaviour can be held responsible for their actions and disciplined where necessary.

2 Policy elements

Policies are split into specific areas each of which has a statement of the risk the company is exposed to if that specific policy is not followed. The overall approach is then stated together with the specific policies for that subject.

2.1 Classification of Information

Information that is particularly sensitive may not be identifiable as such and consequently not receive the protection it requires. Similarly, information may be inappropriately released to the public resulting in poor publicity or commercial disadvantage.

All information and data managed by Afiniti is to be classified so that all personnel know how it should be treated.

- Afiniti personnel should treat Afiniti and client data as **Confidential** regardless of the form in which it is held, only disclosing it externally when authorised and in the case of client data, adhering to the principles of any non-disclosure agreement.
- Information in any form may only be released for public consumption, after being vetted by an authorised manager to ensure accuracy and appropriateness for public consumption after which it can be classified as "Public".
- All information will be identified as such through an appropriate label or notification indicating one of the following classifications.

The following are classifications applicable to Afiniti information

1. **Public** – Information designed for public consumption such as marketing materials and information held on the company's internet site. This information is freely available to Afiniti's clients.
2. **In Confidence** – Information that is to be shared between Afiniti and its business partners, suppliers and clients such as proposals, project plans, etc. Such information should not be copied or shown to any party for whom it was not originally intended.
3. **Confidential** – General company information which would not put Afiniti at a commercial disadvantage if found in the public domain such as work procedures, forms etc.
4. **Strictly Confidential** – Information that if seen by Afiniti's clients, suppliers and / or business partners would put Afiniti at a commercial disadvantage such as company commercial information, rates, business plans etc. Sensitive or critical information must be secured when not in use, especially outside normal working hours.

If you are unsure of the classification of a specific piece of information then discuss the classification with a member of the leadership team.

2.2 Recruitment

A failure to take proper precautions at time of recruitment may result in the employment of unsuitable or unqualified personnel.

Managers must ensure that recruitment procedures are put in place which verify the identity, qualifications, ability, and suitability (e.g. character, credit status) of new personnel.

- Character and/or employment references should be obtained and verified.
- Where academic and professional qualifications are used in support of a job application the originals should be available and may need to be verified. Where they are necessary for a particular role, copies should be held on the individual's personal file.
- An independent identity check, e.g. passport or other document with photograph and address, should be obtained.
- In sensitive posts a credit check and/or CRB check may be required. For personnel holding considerable authority these checks should be repeated regularly.
- In addition to applying the above checks to new starters, it may be appropriate to review some or all of them when an Afiniti personnel is transferring to another role.
- Afiniti personnel with specific information security responsibilities (e.g. security administration) must be qualified and / or received the necessary training.

2.3 Asset Management

Assurance of adequate protection of assets is not possible unless these assets have first been identified. Without records of assets, recovery of losses, say in the event of a disaster, may be difficult or impossible.

- Information assets include but are not limited to physical assets (e.g. computing devices, network equipment, storage media), software assets (e.g. licenses, installation CDs), and data (e.g. stored on PCs, servers, etc.).
- Inventories for all important IT and information assets must be kept and checked regularly for accuracy.
- Records of loans or other movements of valuable or attractive items (e.g. laptops) will be maintained.
- Attractive items such as laptops and other similar portable systems which are easily stolen or misplaced will be assigned to users who will be accountable for the security of the item and information stored thereon. Cost of replacement items could be borne onto the user.
- Equipment for disposal must have all data wiped and licensed software removed.

2.4 Physical Security

Inadequate protection of physical assets, including computers, mobile devices and storage media, may result in systems damage and / or loss of valuable information.

Equipment must be protected from physical security threats and environmental hazards, e.g. fire, smoke, water, dust, theft, tampering, etc.

- Information systems supporting critical or sensitive business activities that is not routinely backed-up our cloud software (e.g. Microsoft 365) will be located in secure areas to which only authorised personnel will have access.
- Equipment must be protected from electrical failures where such failures may cause unacceptable interruption to business operations.
- Equipment supporting critical business operations e.g. Physical servers in London office and the data centre should be protected by an uninterruptable power supply (UPS) which should be tested regularly.
- All reasonable efforts should be taken to protect networks against interception and damage.

2.5 System & Data Backups

A lack of documented user and systems administrator backup procedures or insufficient backups and testing of backups can lead to a loss of data.

Afiniti personnel will be advised as to where to store their data for it to be included in backup processes. Backup processes will be documented and reviewed and tested to ensure integrity of backups.

- Users are responsible for ensuring that all business information is stored in the correct locations on company systems where they are backed up centrally e.g. Microsoft 365
- Where devices are being used remotely, e.g. laptops or PCs for remote workers, data should be in folders which synchronise automatically with our external backup e.g. Microsoft 365. Associates using their own devices should use our external backup as a default workspace, storing and working on documents there.
- Servers such as the T-drive are backed up on a nightly basis.

2.6 Malware

A failure to protect IT assets from potentially damaging software programs such as viruses, Trojans, worms etc, can lead to systems unavailability and the potential loss of confidential information to a third party.

Detection and prevention controls to protect against malicious software (Malware) will be implemented.

- All Afiniti personnel will be made aware of the risks of phishing and malicious software and websites, how to protect from infections, and how to report actual or suspected infections.
- All Afiniti PC's and laptops, and vulnerable servers will have antivirus software installed which is configured to automatically check all data access to and from that machine and to update automatically.
- All non-Afiniti desktops and laptops must have antivirus software installed, kept up to date and set to update automatically.
- All Afiniti personnel must have software firewalls enabled on laptops/desktops. Technical Support will ensure that the antivirus software installed on each Afiniti device is kept up to date. It is the responsibility of Afiniti personnel using non-Afiniti devices to ensure antivirus is installed and kept up to date.
- Software which is no longer used on any device should be removed, disabled or uninstalled.
- Free software (Freeware) should rarely be used as security updates and bug fixes are hard to track and may leave the device upon which they are installed open to Malware attack.
- The 'auto play' or 'auto run' setting which automatically runs software on an external storage device such as a USB stick must be disabled.
- On Smartphones, only approved applications must be downloaded i.e. applications from an app store
- If Afiniti personnel wish to install non-standard software they must first seek permission. If the application is from an approved App Store or vendor and will aid their work then the request should be approved.

2.7 Internet Access

User behaviour on the Internet can be inappropriate and bring the company into disrepute.

Users will be made aware of their responsibilities on the Internet.

- All reports of inappropriate use of the Internet on a device used for Afiniti business containing obscene, racist or sexist information or containing information likely to bring the company's reputation into disrepute will be investigated and, if may result in disciplinary action.

2.8 External Network Access

A failure to control access to internal and external networks may result in loss of information to unauthorised users.

Afiniti technologies including firewalls, proxy servers, VPN and routers will be employed to enforce access control policies. A firewall will be used to control communications between internal company networks and external public (e.g. Internet) networks.

- Network diagrams showing the logical location and connection of systems and network devices will be maintained and reviewed regularly for accuracy.
- Servers and services on the network will be protected by firewalls in groups classified as Internal, DMZ or External.
- All network appliances should have their default settings reviewed at installation and changed if necessary.
- Where possible and practical, data sent over the internet should be encrypted.
- External network security should be reviewed by an independent expert on a periodic basis.

Non-Afiniti technologies such as routers with active firewalls used at home

- Home routers should have their default settings reviewed at installation and changed if necessary i.e. if the password is easily guessable
- The password on internet routers or hardware firewall devices should be at least 8 characters in length, contain both alpha and numeric characters and difficult to guess i.e. not related to names, birthdays etc.
- By default, most firewalls block all services from inside the network from being accessed from the internet – this should be checked in your firewall settings and action taken if not the case.

2.9 Systems Access, User IDs and Passwords

Inadequate system access controls can lead to unauthorised access to information, fraud, or corruption of data. Without a strong access control system and high levels of personnel awareness there will be insufficient accountability for system accesses or changes.

There will be a formal user registration and de-registration processes for access to the Afiniti Network. This includes the allocation, suspension and revoking of user IDs for all users including new personnel, leavers, transfers and name changes.

2.9.1 Systems Access

- All access will be based on the user's operational requirements as authorised by their manager.
- The creation, amendment and deletion of user accounts on the network, systems and services will be managed by Technical Support.
- All IT systems will have appropriate access controls. The controls will uniquely identify and authenticate each authorised user.

- The allocation of special privileges (e.g. Administrator access) will be controlled and restricted to named individuals and they will only use those accounts to carry out administrative activities – standard user accounts must be used for standard operational work.

2.9.2 User IDs

- Every authorised user of the Afiniti network, systems and services will be issued with a unique user name and password.
- Every authorised **business** user of the Afiniti network should access using a regular 'user' account on their laptop/desktop and *not* an administrator account.

2.9.3 Passwords

- Afiniti personnel must comply with the current standards on workstation and password security, and must never reveal their passwords, or allow anyone to use their user account.
- Passwords should be a minimum of 8 characters and contain a mixture of characters and numbers (6 characters for smartphones and only numeric is sufficient). Passwords for primary applications such as Microsoft Office 365 and Salesforce will prompt you for changes periodically.
- Systems should allow users to select their own password and to change it at will.
- Mechanisms or procedures will be in place to ensure that users are immediately forced to change temporary passwords on either first accessing their account or when a password has been otherwise reset.
- If it is suspected that a password bearing system may have been compromised, the company may enforce that all user password expire and require changing with immediate effect.
- User IDs, passwords and details of the system to be accessed will not be sent together using the same method. E.g. system details can be sent by email with user ID and password being sent by text.
- All system administrator accounts will have their default passwords changed.

2.9.4 Unattended Equipment

- All devices must have an automatically activated screen locking facility that is activated whenever the device is not used for a period of time – usually 2 to 10 minutes, depending on the device and operational requirements. Personnel must either log off or lock their Computing devices (including laptops, desktops, mobile phones and tablets) at any time they are unattended.
- Where devices do not support password-protected screen-savers users should log out of active programs before leaving them unattended at any time.

2.10 Mobile Computing

Mobile equipment is particularly vulnerable to loss or theft by nature of its portability and 'attractiveness'. Unless specific attention is given to this increased vulnerability valuable information as well as equipment may be lost.

Users will be given specific guidelines for the use and protection of mobile equipment.

- To guard against opportunistic theft in public places, mobile equipment must be secured out of sight when left unattended e.g. in a locked room, put away in lockable cupboards or drawers or locked in car boot/trunk.
- Backups of information must be made on a regular basis in line with current company guidelines of where information of that type is required to be stored.
- Laptops should have encryption at rest enabled where it exists e.g. Bitlocker on Afiniti laptops with Windows 10 or higher and FileVault on Mac computers.

2.11 Systems Design

Unless security is considered as an integral part of systems design, enhancement and procurement, then major 'holes' that are too difficult or too expensive to fill may result. This could lead to fraud, corruption, unauthorised disclosure or loss of information.

An analysis of security requirements will be carried out at the design and requirements specification stage of any systems project. This includes the development of systems and selection of application packages, utilities, system tools, operating systems, and infrastructure.

- Risk assessments will be undertaken collaboratively by clients, business representatives and application development / technical support staff.
- Systems developed for Afiniti use must comply with the security standards in this policy document.
- Systems developed for Afiniti clients must comply with that client's security requirements as long as they are not in direct conflict with the security standards in this policy document.

2.12 Testing

Unless protected from the errors and risks inherent in untried test environments, information which is normally well protected may inadvertently be lost or corrupted.

The use of live data for testing will be controlled to prevent unauthorised amendment, disclosure or infringement of rules under the Data Protection Act.

- Testing of systems, applications and data changes will be conducted in development and test environments before being implemented onto production systems.
- Successful implementation of systems, applications and data changes will be verified with the user once moved into a live environment.
- Movement of new or amended systems, services and facilities between test and live environments will be planned, managed and authorised using the change control process applicable to that system.

- Copies of live data used for development and testing must be given same level of protection as live system against unauthorised access.

2.13 Change Management

A failure to control implementation and maintenance of new or updated software and hardware may result in system failures or corrupted information.

An effective change control system must be defined and implemented across all areas. This includes the design, programming, implementation and maintenance of computer hardware (e.g. installation of servers, PCs, etc.) and software (e.g. applications, data, operating systems, etc).

- A Management authorisation process for the installation implementation or upgrading of IT facilities must be in place and the process must ensure that a valid business requirement exists.
- New hardware and software should be compatible with existing systems and adhere to agreed Afiniti standards.
- Change control procedures will include regression and / or contingency plans to deal with unexpected failures.

2.14 Business Continuity

Without sufficient plans to deal with unexpected loss of information or IT resources, the business may be unable to carry out critical business functions in the event of a major security breach or a disaster.

Afiniti leadership must consider the need for business continuity plans and, where appropriate, develop mechanisms for ensuring that operational work can continue if key elements of the computers or information systems upon which they rely become unavailable.

- To ensure they are effective, business continuity plans will be tested in accordance with schedules agreed between IT and the business units and as defined in service level agreements.
- Continuity plans should be reviewed for accuracy and completeness on an annual basis or whenever major changes (which could affect the plans) have been made.
- The requirement for contingency plans should be reviewed for any new system introduced to the company.
- The contingency planning process should include appropriate education of Afiniti personnel.

2.15 Legal Requirements

A failure to comply with legal, statutory and regulatory obligations could result in fines or the criminal prosecution against the company, its Directors or its personnel.

To avoid breaches of statutory, criminal or civil obligations Afiniti will take steps to ensure compliance with all aspects of legislation and other regulations affecting the use of information and information systems.

- Afiniti personnel will be made aware of and trained in legislation applicable to information security e.g. GDPR and be expected to conform to that legislation in all circumstances.
- Software will be purchased and used in accordance with its license.
- Software licenses and original software media will be held by Technical Support.
- Afiniti reserve the right to monitor e-mail and Internet activity on its hardware. Such monitoring must take into account local legislation that may prohibit such monitoring or require Afiniti staff or partners to be notified in advance.
- Where a breach of duty or illegal activity is suspected, Technical Support personnel will be authorised to investigate misuse of e-mail, internet systems and networks.
- Management approval should be sought by users before they use information or IT facilities for non-authorised or non-business use.

3 Version History

Version	Created	By	Changes from previous version
2.4	22/02/2018	Jay Dixon	Updated post Cyber Security Assessment and to reflect Afiniti Consultants LLP
2.5	20/03/2018	Jay Dixon	Updated post a review from founder partner, Nick Smith
3.0	27/07/2018	Jay Dixon	Major update for publish to website post GDPR