Information Security Policy

Author:	James Dell
Date:	06/12/2018
Version:	1.1
Document Reference:	Information Security Policy

01235 433 900

80F Park Drive, Milton Park,
Abingdon, OX14 4RY

support@planet-it.net

Document Change Control Sheet

This document will be maintained under change control.

Document Title	Information Security Policy
Version	1.1
Document Reference	PIT007
Date of Last Creation	11/01/2018
Date of Last Issue	06/12/2018
Author	James Dell

Document Distribution

Revision	Date	Author	Comments
1	11/01/2018	Louise Scaysbrook	Initial Draft
1.1	05/12/2018	James Dell	Updated to new format

Revision Details

Revision	Date	Author	Comments
1	11/01/2018	Louise Scaysbrook	Initial Draft
1.1	05/12/2018	James Dell	Updated to new format

Document Approval

Position	Name	Signature
	Louise Scaysbrook	

Contents

01235 433 900

80F Park Drive, Milton Park,
Abingdon, OX14 4RY

support@planet-it.net

1 Policy

INTRODUCTION

Background

This Information Security Policy is based upon the International Standard ISEC/ISO 27001 the Code of Practice for Information Security Management and ISEC/ISO 27002.

Requirements for Policy

Planet IT Limited (hereafter referred to as the Company) has an obligation to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS) to all staff, suppliers and partners.

The objective of this requirement is to ensure that users of IT/IS facilities do not unintentionally place themselves, or the Company, at risk of prosecution or disciplinary action, by carrying out computer related activities which contravene current policy or legislative restrictions.

Information within the Company is intended to be openly accessible and available to all members of the organisation for sharing and processing. Certain information (sensitive information) has to be processed, handled and managed securely and with accountability.

This policy outlines the control requirements for all information contained within the Company network and IT systems.

Policy Structure

This document forms the Company's Electronic Information Security Policy. Its purpose it to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Company.

Supporting policies and guidance documents containing detailed Information security requirements will be developed in support of this policy. Dependent upon the subject matter, supporting policies and guidance will either apply across the Company or to more specific groups or individuals within the Company.

Purpose and Scope

All processing of data and collection of information will be processed in accordance with UK law.

This policy defines how the Company will secure electronic information, which is found within:

- The Company's IS/IT infrastructure.
- Key Business System data and information.
- Security of information held in electronic form on any Company computer.

And is processed or used by:

- Company Staff and suppliers who have access to or administer the Company network or IT systems.
- External users, agents, and guest users authorised to use the Company network or IT Systems.
- Individuals who process key data and information within Key Business Systems.

Objectives

Information Security controls are designed to protect members of the Company and the Company's reputation through the preservation of:

- Confidentiality – knowing that key data and information can be accessed only by those to do so;
- Integrity – knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- Availability – knowing that the key data and information can always be accessed.

The Company is committed to protecting its members and Key Business Systems. Controls will therefore be deployed that mitigate the risk of vulnerabilities being exploited which adversely affect the efficient operation of the Company.

Applicability

This policy applies to all users of the Company network and IT Services and includes:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of, the Company;
- Suppliers working at the Company;
- Third party contractors and consultants working for or on behalf of the Company;
- All other individuals and groups who have been granted access to the Company's network or IT Services.

These categories of persons and agencies are collectively known as the 'user' in the policy document.

The Directors of the Company are ultimately responsible for ensuring that adherence to this policy is observed and for overseeing compliance by users under their direction, control or supervision.

Each user is responsible for their own actions and must ensure all actions relating to using the Company network and IT Services adheres to the principles and requirements of this policy.

LEGISLATION AND POLICY

Legislation

Supply and use of the Company network and IT Services is bound by UK law.

Associated Policies

The Company is also governed by external policies which impose responsibilities on the provision of IT Services and network access.

The principles in this policy support and enhance the requirements contained within these documents and ensure compliance with contractual agreements.

INFORMATION SECURITY – RISK MANAGEMENT

Information security governance is the structure which supports the implementation of this policy. An IT infrastructure will be implemented within the

Company to ensure the effective and efficient implementation of this policy across the Company.

Ownership and Maintenance of Policy

This policy is owned by the Company and is maintained, reviewed and amended by the IT Manager in accordance with Company policy, procedures and guidance.
This policy will be subject to annual review.

Risk Management and Electronic Service Incidents

The Company will be responsible for raising an incident message in relation to any reported security incident at the Company. These incidents will be recorded as 'Electronic Security Incidents'.

Electronic Security Incidents will be recorded with a unique reference number. A review of incidents will be conducted at six monthly intervals. Incidents considered to be exhibiting unacceptable levels of risk to the Company network or IT Services will be subject to an investigation to identify the inherent vulnerabilities exposed by this incident. A report will be submitted to the IT manager for consideration of the question of suitable remedial action which may be effectively implemented to mitigate future risks.

Security of Third Party Access

Procedures will be developed to regulate access to the Company's information processing facilities by third parties. Such access will be controlled and regulated in order to protect information assets and prevent loss or damage to data through unauthorised access. The IT Manager will consider applications for access to facilities by contractors or third parties based upon a risk assessment of the proposed task.

Identification of Risk from Third Party Access

Third parties who require access to the Company's IT/IS infrastructure will be bound by contracts which define Company security requirements. Prior to being granted any network connectivity they will be required to sign and undertaking to adhere to the requirements of the Company policy and where sensitive information or sensitive business / research information is involved they will be required to sign a non-disclosure agreement prior to access to the IT network.

ASSET CLARIFICATION

Information assets will be categorised and recorded to enable appropriate management and control.

Inventory of Assets

The Company will maintain an inventory, subject to audit, or IR related assets.

For each item, the inventory will state the item's description, make, model, serial number and/or service tag and location. This inventory is in addition to asset records maintained under Company financial regulations.

Any system and the data it contains that is not part of the above inventory is the responsibility of the creator of that system. However, the asset will require compliance with this policy and users will be required to adhere to the principles of this document.

All asset identification procedures must be compliant with and support the Company Business Continuity Plan

PERSONNEL SECURITY ISSUES – ROLES AND ACCESS LEVELS

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

The Company maintains a directory of people and suppliers which are authorised to use the Company network, IT services and applications. All users, staff, suppliers, external users and guest users are subject to the principles of this policy and must certify that they agree to the terms.
If a user's relationship with the Company alters, due to a change in role or employment relationship, then the revised level of access must match both the new role and relationship with the Company. All IT account access levels must comply with the requirements of the Company policy.

Security in Job Descriptions

Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection

of particular assets, or the execution of particular processes or activities such as data protection.

Confidential Personal Data – Sensitive Information

All data which identifies any individual will be handled in accordance with the Data Protection Act 1998. All personal details will be held securely and in accordance with current UK legislation.
All data classified as sensitive data will be processed and stored in compliance with the current sensitive information guidelines and Company policies and procedures.

Confidentiality Undertaking

All suppliers, members of staff and partners are reminded of their obligation to protect confidential information in accordance with the Company's standard terms and conditions of employment.

All users will be bound by the confidentiality agreement in either their contract or terms of employment.

Employee Responsibilities

All staff (including agency and casual staff) must agree to written terms and conditions contained within the Company policies when they register to use an IT service.

The Company shall ensure that:

- Confidentiality agreements form part of the terms and conditions of employment;
- Awareness training about electronic information security forms part of Company staff induction programmes;
- Information for all staff on electronic information security is maintained in the Company information;
- All references for a period extending to three years prior to the recruitment date are checked by personnel prior to a member of staff's commencement of employment.

The Company must ensure that where there are specific security roles and responsibilities they are documented in all relevant job descriptions and that there is appropriate screening of applicants.

Staff Leaving Employment

On termination of employment with the Company, any applicable user accounts, accesses and passwords will be changed or removed. Except where a strong business case exists, which meets the needs of the Company, all user accounts will be closed at the termination of employment. Files and folders will be deleted shortly after the user leaves the Company.

Responding to Security Incidents

Suspected Security Breach

Staff of suppliers using or administering the Company network or IT Services must not in any circumstances try to prove or collect evidence in relation to any suspected or perceived security breach. The exception to this rule is where staff has been granted a specific policy exemption which allows them to do so as part of their role. The IT Manager will be responsible for identifying members of staff who are responsible for security breach investigations.

A security incident is any incident which alters, destroys or amends data within the Key Business Systems without authority. This may cause damage to or reduce the efficiency of the Company network or IT Services. This includes any actions or behaviours which contravenes Company policy, statutory or common law, legal requirements or professional regulation or guidance.

Reporting Security Incidents

All suspected security incidents are to be reported in the first instance to the IT Manager.

Initial reports of suspected security incidents should be channelled through their Line Manager to the IT Manager. Alternatively, to the Company Directors under the provisions of the Company whistle blowing code of practice.
All reported security incidents and active investigations will be monitored by the Company Directors. An appropriate investigation and action plan will be prepared and agreed with a representative of the Company Senior Management Team.

Within the provisions of the UK Law, the Company reserves the right at an time to intercept and monitor communications in accordance with the Regulation of Investigatory Power Act; The Telecommunications (Lawful Business Practise) (Interception of Communications) Regulations. The above legislation will be implemented in compliance with the Company monitoring provisions.

Monitoring and recording of electronic communication and data will be carried out in accordance with current Company Policy and interception / monitoring of individual activity shall normally only take place with prior express approval of the Company Directors, but may be undertaken without any prior notice to the users of the Company systems. Permission for undertaking monitoring or surveillance of user activity may in the first instance be given verbally. Any such permission must be recorded in writing as soon as practical. This requirement is to ensure an auditable investigatory process exist for an subsequent disciplinary or criminal proceedings.

Security Incident Management / Investigation

The senior member of staff identified as being responsible for investigating the incident will ensure that all steps are taken to limit damage and loss of data whilst preserving the reputation of Planet IT Limited.

The IT Manager will maintain written procedures for the operation (e.g. start up, backup, show down and change control) of those Company Key
Business Systems where threat, risk and organisational impact would adversely the operational effectiveness or organisational reputation.

Investigating Information Security Incidents.

On receipt of information indicating that a security incident may have taken place, the IT Manager will nominate a member of staff to coordinate the investigation.

Network Isolation and Reconnection

Any device perceived as placing the integrity of the Company IT network at risk of harm or service interruption will be isolated from the main network.

Suspension of network connectivity will remain in force until the issue has been investigated and a plan of action agreed with the IT Manager to resolve the issue.

Subsequent reinstatement will only be permitted once the requirements of that action plan have been met, verified and authorised by the IT Manager

PHYSICAL AND ENVIROMENTAL SECURITY

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to information assets.

Physical Security

Computer systems and networks will be protected by suitable physical, technical, procedural and environmental security controls.

File servers and machines that hold or process high criticality, high sensitivity or high availability data will be located in suitable area. All Key Business Systems will be subject to security measures which supports the Company Continuity Plan.

Data Storage Facility Security

Access to the offices and server rooms and any locations containing data communications or telephone equipment will be controlled and restricted. Authority to access these areas will be controlled by the IT Manager.

Equipment Security

Servers holding corporate information will be held in a secure environment protected by:

- Physical security and access control;
- Fire detection and extinguishing systems.

External hosting must not take place without prior approval from the Company Executive.

The IT Manager must ensure the IT infrastructure is covered by appropriate hardware and software maintenance and support.

Workstations must be appropriately secured and operated by Company staff who must be trained in and fully conversant with this policy and their personal

responsibilities for confidentiality of information displayed on the screen or in printed output.

Backup media must be retained in accordance with the Company Policy on retention of records and the Data Protection Action 1998.

All Company data must be cleared securely from Company IT equipment and media on disposal. The responsibility for disposal lies with the IT Manager.

COMMUNICATIONS AND OPERATIONS MANAGEMENT

Controls will be implemented to enable the correct and secure operation of information processing facilities.

Documented Operating Procedure

Design, build and configuration documentation will be produced in respect of system platforms. Sensitive documentation will be held securely and access restricted to staff on a need to know basis.

Segregation of Duties

Access to Key Business Systems and key data and information will only be granted based on the user role and access clarification.

When deemed necessary segregation of duties between operations and development environment shall be strictly maintained and all work on Key Business Systems will be strictly segregated.
Permanent and full access to live operating environments will be restricted to staff on role-based requirements.

Sensitive operations will be identified and action taken to implement split functional controls where appropriate.

System Planning and Acceptance

System Changes

All changes to live Key Business Systems will follow a predefined change management process, to ensure that activities are undertaken in accordance with stringent change control processes.

Controls Against Malicious Software

Controls will be implemented to check for malicious or fraudulent code begin introduced to Key Business Systems.

Source code written by contractors and staff will be subject to security scrutiny before being installed on any line Key Business System.

All systems will be protected by a multi-level approach involving firewall, router configuration, email scanning, and virus and spy/malware protection on all workstations on the Company network.

All Company workstations will have the appropriate anti-virus software installed and set up to update anti-virus signatures automatically. This must not be turned off by users with unlocked desktops. Any device found to pose a threat to data or the provision of the Company network will be isolated from the Company network until the security issues are resolved.

Staff and suppliers may use their own PC hardware to connect to the Company WiFi network. Equipment so used will be the subject to security checks and a number of prerequisites before being allowed to establish a connection with the Company network.

Network traffic will be monitored for any anomalous activity which may indicate a security threat to the network.

Virus Protection

A Virus Protection procedure will be implemented to prevent the introduction and transmission of computer viruses both within and from outside the Company. Failure to maintain a device in a state which prevents or detects virus infection will leave the device liable to exclusion from the Company network until the security issue is resolved.

Security Patches Fixes and Workarounds

The IT Manager will be responsible for the day to day management of systems and is responsible for ensuring that security patches, fixes and workarounds are applied in a timely manner to reduce vulnerabilities to devices within the Company network. Such patches, fixes and workarounds must be tested and approved before deployment and the efficiency of the deployment will be

monitored to ensure the effective mitigation of risk due to known vulnerabilities.

IT Housekeeping and Storage

Data Storage

System backups will be performed automatically by the relevant systems or manually by staff in accordance with documented procedures. The procedure will include keeping backups off site. Periodic checks will be made to ensure backup media can be read and files restored. Records of backups will be monitored by the IT Manager and be subject to random audits.

Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual user data files backup and recovery of individual user files is the responsibility of the information owner.

Network Management

Controls will be implemented to achieve, maintain and control access to computer networks, including wireless LANs.

No IT equipment may be connected to the Company network without approval. Any device found to be installed without prior authority will be disconnected, the equipment removed and an investigation commenced to establish the cause of the network compromise. Users should be aware that installation of such devices is potentially a disciplinary and criminal offence under the Misuse of Computers Action 1990.

Devices Disposal

Removable magnetic and optical media containing Key Business System data or Sensitive Information will be reused or disposed of through controlled and secure means when no longer required, in accordance with the Disposal of IT Equipment Advice. Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic (WEEE) Regulations and through secure and auditable means.

Procedures will be made available for the secure disposal of removable data storage media containing Key Business System data or sensitive information when these become defunct or unserviceable.

Software Usage and Control

Software will be used, managed and controlled in accordance with legislative and Company policy requirements in relation to asset management and licence agreements.
All major software upgrades and in-house systems development for Key Business Systems will be appropriately controlled and tested through a managed process before live implementation and deployment.

All software used on devices managed by the Company must be installed in compliance with current software licensing policies. Software installed without prior authority and agreement may leave a user liable to prosecution under the Misuse of Computers Act 1990 and disciplinary action.

INFORMATION EXCHANGE REQUESTS

Use of the Company network will be governed by the Electronic Information Security Policy and the Policy for using IT Resources.

Failure to comply with these requirements will leave a user liable to disciplinary and/or possible criminal legal penalties.

Exchange of Information with Outside Organisations

Requests by external bodies for the provision of electronic information from Key Business Systems will in all instances be referred to the information owner. This includes Data Subject Access Requests made under the auspices of the Data Protection Action 1998.

Requests for information under the Freedom of Information Act will be referred to the Company Directors. All applications will be handled in accordance with the FOI Application Procedure.

ACCESS CONTROL

Policy Statement

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorisations. These procedures shall be implemented

only by suitably trained and authorised staff. A periodic review will be conducted to verify user access and roles.

Planet IT Limited Operational Policy

Access to Key Business Systems will be appropriately controlled and comply with the access rights of the user.
Access to the Company network and IT Services will be restricted according to the access classification of the user.

Company staff, suppliers and external users may use:

- Standard software portfolio;
- Shared file store;
- Email, calendar and public folders;
- Company Business Systems;
- Internet.

Guest users may use:

Standard software portfolio;
Internet (no email account will be issued).

User Responsibilities

Users of the Company network must comply with Company Policies and the Electronic Information Security Policy.

All staff (including agency and temporary staff) must agree to written terms and conditions covering use of IT when they register to use Company IT services.

Personnel Services shall ensure that:

- Confidentiality Agreements form part of the terms and conditions of Employment;
- Awareness training about electronic information security forms part of Company Staff Induction Programmes;
- Information for all staff on electronic information security is maintained in the Employee handbook;
- All references for a period extending to three years prior to the recruitment date are checked by personnel prior to a member of staff's commencement of employment.

The Company must ensure that where there are specific security roles and responsibilities they are documented in all relevant job descriptions and that there is appropriate screening of applicants.

Access to Company systems may be withdrawn and Company disciplinary procedures invoked where a serious or deliberate breach of the policy is made.

Guest Users and Open Access

Guest user accounts and open access facilities may be used to allow visitors strictly limited access to public Company IT. Written records of such IT use (who, when and where) must be maintained by the Company.

Access to corporate systems, protected electronic resources, Company email services and personal file stores will not be permitted for guest users.

Company Key Business System Access

Subject Access Management and Administration

Formal procedures will be implemented for granting access to both the Company network and IT services. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate to the role and relationship with the Company. Accounts identified as dormant will be closed in accordance with current procedures.

Remote Access

Controls will be implemented to manage and control remote access to the Company's network and IT services.

Users should note that failure to comply with Company policies will leave the user liable to disciplinary action and possible criminal law prosecution under the appropriate legislation.

Mobile Computing

The Company recognises the inherent dangers of information stored on portable computers (laptops, notebooks, tablets and smart phones) as well as removable media. The Company will provide security advice to staff as requested. The advice is issued as a guideline for users and failure to follow

recommended guidance will leave a user vulnerable to disciplinary action should Key Business System Data or sensitive information be lost or altered. Wireless computer networks potentially introduce new security risks.

Password Management

Users are required to follow good security practices in the selection, use and management of their password and to keep them confidential.

Primary access to the Company network and IT services is governed by a network username and password giving access to a set of network services.

Authorisation of access to Key Business Systems and to the data held by them is the responsibility of the system owner.

The control of network passwords is the responsibility of the IT Manager. Network passwords are stored in encrypted form.

System administrator passwords will be issued on the express authority of the IT Manager on a need to know basis. Such password will be changed regularly and when authorised systems administrator staff leaves.

For Windows Operating Systems the following must be enforced:

- Network password must be a minimum of six characters;
- Network password will be subject to enforced periodic change. The life of a chosen password will be six months;
- Network password history will prevent reuse of the last three password changes;
- Accounts will be locked on the third failed log in attempt.

Policy on network password complexity will be reviewed periodically.

The IT Manager must be notified when staff leave and will be responsible for closing the associated accounts.

The account type should at all times reflect the business relationship existing with the member of staff. As a staff member moves to a less formal relationship with the Company then the account associated with that person should reflect this new relationship.

The Company will maintain a list of staff with access to key business systems and services. A password matrix will be maintained to ensure business continuity

and mitigate risk. This password matrix will be kept securely to ensure swift response to critical incidents.

Unattended User Equipment

Users of the Company network and IT services are responsible for safeguarding Key Business System Data and sensitive information. In order to protect these information assets, users are required to ensure that devices are not left logged on when unattended and that portable equipment in their custody is not exposed to opportunistic theft, unauthorised access or observation of sensitive information.

Where available, password protected screensavers and automatic log out mechanisms are to be used on office based systems to prevent individual accounts being used by persons other than the account holders, but not on cluster computers that are shared by multiple users.

Users will utilise the following security features of the system:

- Logging out of sessions when the session is finished;
- Logging out of sessions when a computer is to be left for more than fifteen minutes;
- Whenever possible and at the end of the working day, switch off computers when not in use.

Users are required to follow the guidance on user responsibilities and Personal Responsibilities for Electronic Information Security. Failure to adhere to these recommendations will leave the user liable to possible disciplinary or criminal prosecution.

Monitoring Systems Access and Use

Access to and use of the Company network and IT systems will be monitored in accordance with the provisions of the Policy for Using IT Resources.

Remote access by third party contractors to maintain and support Company IT systems will be subject to appropriate monitoring and control measures defined by IT services. Third party access will only be granted where the applicant has agreed to the terms and conditions of the ICT Acceptable Use Policy.

COMPLIANCE

Compliance with Legal and Company Policy

Supply and use of the Company network and IT services is bound by UK law current at the time of any reported incident. The policy for using IT resources provides guidance on the most common legal and policy requirement pertaining to Company network use.

Guest users may be permitted limited right to use IT services The Company will review this policy periodically.

The IT Manager will maintain and monitor, at six monthly intervals, reports of records of electronic security incidents. Reports will be considered by the Company. It will then be decided id further action or investigation is required.

The IT services password matric, listing members of staff with access to key systems and services, will be maintained by the IT Manager and the master copy held in a secure public folder.

People who are neither staff nor suppliers do not normally have an automatic right to use the Company network or IT services. Authorisation for such external users will be subject to sponsorship from a member of Company staff along with written agreement from the user to abide by the Company policies.

All applications for external users will be subject to approval by the Company Directors or nominated representative.

Any outsourcing must include express provisions with respect to IT security and control and any applicable UK law in relation to data processing and confidentiality.

I agree that I have read and understood this policy and will abide to it.

Employee Signature: _____

Printed: _____

Date: _____