Information Security Policy

Version: 1.4

22 September 2017

Document History:

Version	Date	Description (Changes made)	Author
1.0	28/10/16	Document created	Charlie Lines
1.1	03/05/17	Updated recommend password security	Charlie Lines
1.2	24/05/17	Updated to include GDPR reference	Charlie Lines
1.3	06/07/17	Updated Business Continuity plan link	Charlie Lines
1.4	22/09/17	Updated links to associated documents	Reuben Sutton

Document References:

Reference	Version	Title	Author
B4MZ	Versions	Business Continuity Plan	Charlie Lines
ARKB2490507	Versions	Recommended Password Security	Charlie Lines
ARKB2490623	Versions	Equipment reuse or disposal	Charlie Lines
ARKB2490755	Versions	About laptop encryption	Charlie Lines
ARKB2490817	Versions	Safe internet use	Charlie Lines

Document Review & Approval

Name	Date	Version Approved/Comments
Charlie Lines	23/10/17	1.4 CL
Reuben Sutton	23/10/17	1.4 DL

1. Introduction

1.1. Purpose and Scope

This document defines the Information Security Policy (ISP) for Plandek.

It defines the approach to be taken to manage information security in order to ensure that our information assets are properly protected against a variety of threats. It also outlines the policy for the protection of the confidentiality, integrity and availability of Plandek's information assets.

The purpose of this document is to:

- Ensure that Plandek's information is protected against unauthorised access, disclosure, change or loss, is accurate, up-to-date and is available when required;
- Ensure effective and timely implementation of information security throughout Plandek;
- Raise awareness of information security issues within Plandek; and
- Minimise damage or disruption by preventing and reducing the impact and exposure of information security incidents.

This Information Security Policy applies to all Plandek staff including Plandek permanent staff, long term and short term part time employees, secondees, partners, volunteers, co-located personnel, visitors and relevant identified third parties accessing Plandek's information resources.

This Information Security Policy provides a framework of supporting policies, procedures and guidelines designed to ensure that Plandek's information remains confidential, accurate and available for its proper purpose.

1.2. Document Ownership, Maintenance and Review

The document is owned by the Plandek COO. The Plandek COO has direct responsibility for maintaining this policy, providing advice and guidance on its implementation and is responsible for ensuring that this policy is reviewed annually and updated and communicated accordingly.

2. Objectives of Information Security

The primary objective of information security is to minimise business damage by preventing and minimising the impact of information security breaches and incidents and therefore protecting the reputation of Plandek.

The objective of this document is to establish the policy for the protection of information in any form, held, obtained, recorded, used or shared by Plandek, its partners and its stakeholders to ensure the security of our collective assets, so that the following apply:

Confidentiality: The protection of valuable or sensitive information from unauthorised disclosure or amendment will be assured;

Integrity: Protection against unauthorised modification will safeguard the accuracy and completeness of information; and

Availability: The processing of information will be appropriately authorised and accessible to users when required.

2.1. What is Information Security?

Information is an asset that, like other business assets, has a value to the organisation and consequently needs to be protected. Information security protects information from a wide range of threats, accidental or intentional, in order to ensure business continuity and to minimise business damage. It can be characterised as the preservation of confidentiality, integrity and availability.

Whatever our job, we all work with information in many forms, information shall mean any content whatever its medium (written on paper or stored in electronic form) e.g. computer systems, hard copy reports and correspondence, and it is up to each of us to protect it appropriately.

2.2. Why is it needed?

Plandek's information and the systems, on which much of the information is stored, are important and often critical business assets due to their commercially sensitive nature.

Plandek not only holds its own sensitive information but we also receive sensitive information from various external sources including our customers. Such information needs to be protected from unauthorised disclosure.

Information is at risk from errors, natural disasters, fraud and other accidental or intentional events. Plandek cannot pursue its business effectively and efficiently if reliable information is not available when needed.

To fulfil our commitments to our customers, Plandek must take action to mitigate the impact of disruption from internal and external sources. The key objective is to maintain a practical and robust response to unplanned events that impact the ability of Plandek to meet its responsibilities.

3. Information Security Policy Statements

Plandek is committed to maintaining and improving information security and managing exposure to information security risk. It is therefore mandatory policy to ensure that the following baseline minimum controls are implemented:

Information Security

- All staff must be responsible for information security and therefore must understand and comply with this policy. Plandek would view a failure to comply with this policy as a serious matter that could be treated as a disciplinary offence.
- All Plandek permanent staff, long term and short term part time employees, secondees, partners, volunteers, co-located personnel, visitors and relevant identified third parties working with Plandek's information and systems must be responsible for ensuring the information security of all information for

which they are directly or indirectly responsible or handle in any way. They are expected to be aware of this Information Security Policy and may be accountable for any information security incidents.

- Information security requires the participation and support from all staff (Plandek permanent staff, long term and short term part time employees, secondees, partners, volunteers, co-located personnel, visitors and relevant identified third parties working) who must be provided with sufficient information security awareness training and supporting procedures to allow them to properly protect and manage Plandek information.
- Supporting procedures must be provided to allow staff to properly protect and manage Plandek information, such as office, home and mobile working procedures.
- Information security risks to Plandek must be identified and managed.
- Information (however stored) must be protected against unauthorised access.
- The confidentiality of information must be assured.
- The integrity of information must be maintained.
- The availability of information must be ensured as required by the business process.
- All breaches of information security, actual or suspected, must be reported to the Plandek COO and investigated accordingly.
- All system developments must include information security controls in the system development lifecycle.
- Proposed projects must be subject to a high-level information security risk assessment that requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.
- Proposed system implementations must be subject to appropriate security testing activity.
- All new information systems, applications and networks must be approved by the Plandek COO before they commence operation.
- Individuals' access to systems required by their job function must be appropriately controlled.
- Department managers are responsible for authorising remote access for telecommuting workers, sales personnel and others with a valid business need.
- Staff requirements for remote access should be reviewed on a regular basis.
- An audit trail will be recorded for their remote access sessions.
- Information security responsibilities must be documented in commercial third party contracts.
- Third parties who process Plandek information and/or provide information services to Plandek shall be identified and, where the category of sponsor or supplier is deemed appropriate by Plandek, shall be accountable for developing their information security frameworks in line with the Plandek Information Security Policy.
- Third parties must identify a point of contact or representative for information security, develop information security policies and associated procedures and pro-actively identify and manage information security risks. Plandek has the right to audit and review information security arrangements of third parties.

Two-factor Authentication

- To reduce the risks of information leakage, unauthorised access and damage to confidentiality, two-factor authentication is mandatory for all staff accessing AWS, Google Cloud and GitHub. Two-factor

authentication adds that extra layer of security by forcing you to use something you have (e.g. key fob or mobile device) to verify your identity.

VPN

- To allow for greater security when accessing potentially secure resources from home Plandek requires the use of a VPN. This allows the remote user to connect and have their computer act as if it is sitting at the office.

Third Party Access

- Access to information resources and computer systems by third parties must be strictly controlled and be authorised in advance.

Human Resources

- Plandek staff must be informed of their information security roles and responsibilities as part of the recruitment process.

Legal

- Plandek must comply with all applicable laws and regulations governing information security.
- Plandek staff should understand and comply with their obligations under the Data Protection Act and the General Data Protection Regulation (GDPR). Both give protection to personal data, relating to living individuals, held in certain types of manual files as well as that processed by computer. Plandek will consider staff to have committed a serious disciplinary offence if they knowingly fail to handle personal data according to the principles of the Data Protection Act or GDPR.

Clear Desk and Printers

- To reduce the risks of information leakage, unauthorised access and damage to confidentiality, sensitive hardcopy material must not be left out unattended where it could be read on desks and printers. Staff will receive appropriate training on the secure handling and printing of sensitive documentation.

Secure Disposal

- Shredders must be used for all sensitive information.
- Electronic media must be clearly erased or destroyed prior to disposal. It is vital to use the appropriate procedure for the safe and secure disposal of electronic media that is deemed defective or obsolete.

Business Continuity

- All staff must understand Plandek's Business Continuity response[1]; when and how it is activated, what to do and where to go in order to continue to meet our responsibilities.

[1] https://3.basecamp.com/3410018/buckets/3887913/uploads/743755842

4. Personal Responsibilities

Information security requires the participation and support from all staff. A number of relevant DOs and DON'Ts on information security best practice to be followed by all staff with immediate effect are summarised in this section.

DO'S

- Ensure that all documents are promptly removed from printers and fax machines.
- Ensure that the appropriate disposal procedure is followed when dealing with disposal or reuse of equipment.[2]
- Ensure that the contents of your laptop are encrypted.[3]
- Use shredders for all confidential and sensitive information.
- Ensure you are responsible for the safekeeping of your login password.
- Do keep your password private.
- Ensure you always check for correct content, attachments and recipient names before sending e-mails.
- Ensure at the end of each day, that all sensitive information is removed from the work place and stored in a locked area. This includes business critical information such as contracts, or sensitive client information.
- Where lockable safes, filing cabinets, drawers, cupboards etc are not available, office / room doors must be locked if left unattended.
- Ensure that sensitive data is always sent encrypted when sent via the internet.
- Ensure appropriate security policies are used on hosting environments
- Ensure named accounts are in use on all Plandek secured systems, including our platform.
- Ensure periodic reviews take place of accounts on Plandek systems to ensure access is appropriate.
- Ensure access is restricted by IP address between platform systems and third parties.
- Do exercise caution when using the internet and follow safe internet use guidelines.[4]
- Do exercise caution with the use of any portable media (including memory sticks or cards) and ensure that all files contained on media or devices is scanned with an anti-virus program before use.
- Ensure that all passwords, created or maintained by yourself, are in line with the Plandek password policy, particularly on minimum length and complexity.[5]
- Contact the COO if you are ever in doubt about security.

DON'TS

- Don't allow any person you don't know to 'shadow' or 'tailgate' you to gain access to premises.

[2] https://3.basecamp.com/3410018/buckets/3887913/documents/743896466
[3] https://3.basecamp.com/3410018/buckets/3887913/documents/743897334
[4] https://3.basecamp.com/3410018/buckets/3887913/documents/743897831
[5] https://3.basecamp.com/3410018/buckets/3887913/documents/743895663

- Don't use anyone else's user ID and password and never let anyone use yours.
- Don't use passwords that could easily be guessed or deduced.
- Don't open e-mail attachments if they are from an unknown source.
- Don't originate, send, forward, re-distribute or reply to chain letters, junk mail or spam. If you receive a chain mail, do not follow the instructions in the mail. Delete the mail immediately.
- Don't automatically forward Plandek e-mails to your personal e-mail accounts.
- Don't leave your workstation / computer left logged on and unlocked when unattended. They must be password protected.
- Don't download unauthorised executable files / software from the internet as it may contain malicious code or spyware that could lead to an information security breach or compromise Plandek's IT systems.
- Don't leave laptops or other equipment containing potentially sensitive data unsecured in the office overnight. They should either be locked away or removed from the office each night.
- Don't misuse customer information. The disclosure, use or destruction of confidential customer data can have adverse effects on Plandek's relationship with customers, and possibly carry significant liability for both.

5. Reporting Information Security Incidents

An information security incident is deemed to occur whenever there is an actual or attempted breach of the confidentiality, integrity or availability of Plandek's information or information services.

Information security incidents include, but are not limited to:

- Unauthorised access to Plandek information (including hacking attempts and denial of service attacks);
- Theft or loss of Plandek information / IT assets (e.g. laptops, data devices, PDAs);
- Infection of Plandek's systems by viruses or other malicious software (e.g. spyware, viruses, worms or trojans);
- Staff misuse of information systems (e.g. web access and e-mail access); and
- Systems failure, loss of service or data corruption.

All Plandek staff (including contractor and partner staff) are responsible for reporting any suspicious or unusual activity, including any actual, or suspected, information security incidents, in a timely manner to an appropriate manager or to the COO.

6. Summary

In summary, information security is **everyone's** responsibility. Information security has to be embodied into the Plandek culture and as such, it is vital that all of our staff members, secondees, contractor and volunteers have a clear understanding of what is expected of them. They must therefore understand and comply with this policy.

All violations of Plandek's information security policies, standards and procedures must be reported immediately.

Failure to comply with this policy will be viewed as a serious matter, which could be treated as a disciplinary offence, including as an act of gross misconduct.