PROCHAINMATRIX

Security Policy

DOCUMENT CONTROL

Title	Security Policy
Author	Prochainmatrix
Accountable Officer	Security Officer
Unique Identification Reference	SP-P-0519-01
Information Classification	Public
Document Version Number	1.6

DOCUMENT HISTORY

Version	Date	Changes made
1.0	10th May 2019	Document Creation
1.1	14th May 2019	Minor format updates
1.2	4th September 2020	Updated Information Classification
1.3	7th October 2020	Formal Review and fixed document layout and structure.
1.4	21st October 2021	Formal Review. Minor edits to content for clarity.
1.5	4th April 2022	Section 10 update
1.6	1st May 2022	Minor edits, 9.5 heading adjusted to omit ‘local backup’ and clause additions to provide further detail, clause 3.9 added.

1. Introduction

1.1 This information security policy is a key component of the Prochainmatrix management framework. It sets the requirements and responsibilities for maintaining the security of information within Prochainmatrix. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

1.2 Prochainmatrix Limited is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorised access, use or disclosure. All information that we collect is contained behind secured networks and is only accessible by those with the security access level clearance within our company.

1.3 All operating systems and firmware are supported by Redcentric, who produce regular fixes for any security problems as part of their contracted service with Prochainmatrix.

2. Aim and Scope of this policy

2.1 The aims of this policy are to set out the rules governing the secure management of our information assets by:

2.1.1 Preserving the confidentiality, integrity and availability of our business information.

2.1.2 Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.

2.1.3 Ensuring an approach to security in which all members of staff fully understand their own responsibilities.

2.1.4 Creating and maintaining within the organisation a level of awareness of the need for information.

2.1.5 Detailing how to protect the information assets under our control.

2.2 This policy applies to all data, information systems, networks, applications, locations and staff of Prochainmatrix or supplied under contract to it.

3. Responsibilities

3.1 Ultimate responsibility for information security rests with the Chief Executive of Prochainmatrix Limited, but on a day-to-day basis the Security Officer shall be responsible for managing and implementing the policy and related procedures.

3.2 Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by Tasos Yerolemides. Both the Policy and the Risk Register shall be reviewed by Tasos Yerolemides at least annually.

3.3 Line Managers are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:

3.3.1 The information security policies applicable in their work areas.

3.3.2 Their personal responsibilities for information security.

3.3.3 How to access advice on information security matters.

3.4 All staff shall comply with the information security policy and must understand their responsibilities to protect the company’s data. Failure to do so may result in disciplinary action.

3.5 Line managers shall be individually responsible for the security of information within their business area.

3.6 Each member of staff shall be responsible for the operational security of the information systems they use.

3.7 Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

3.8 Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

3.9 Prochainmatrix ensures due diligence is caried out on customer and vendor orders on the appropriate accreditations.

4. Legislation

4.1 Prochainmatrix Limited is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.

4.2 The requirement to comply with legislation shall be devolved to employees and agents of Prochainmatrix, who may be held personally accountable for any breaches of information security for which they are responsible.

4.3 In particular, Prochainmatrix is required to comply with:

4.3.1 The Data Protection Act (2018)

4.3.2 The Data Protection (Processing of Sensitive Personal Data) Order 2000.

4.3.3 The Copyright, Designs and Patents Act (1988)

4.3.4 The Computer Misuse Act (1990)

4.3.5 The Health and Safety at Work Act (1974)

4.3.6 Human Rights Act (1998)

4.3.7 Regulation of Investigatory Powers Act 2000

4.3.8 Freedom of Information Act 2000

5. Personnel Security

5.1 Contracts of Employment

5.1.1 Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.

5.1.2 References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.

5.1.3 Information security expectations of staff shall be included within appropriate job definitions.

5.1.4 Whenever a staff member leaves the company their accounts will be disabled the same day they leave.

5.2 Information Security Awareness and Training

5.2.2 The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.

5.2.3 Information security awareness training shall be included in the staff induction process. The Security Officer will highlight the importance of following company policy and procedure, cover key security policy topics and answer questions during a scheduled meeting with new employees which will be renewed annually.

5.3 Intellectual Property Rights

5.3.3 The organisation shall ensure that all software is properly licensed and approved by the Intellectual Property Office. Third Party and Prochainmatrix intellectual property rights shall be protected at all times.
5.3.4 Users breaching this requirement may be subject to disciplinary action.

6. Access Management

6.1 Physical Access

6.1.1 Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

6.2 Identity and passwords

6.2.2 Passwords must offer an adequate level of security to protect systems and data
6.2.3 All passwords shall be ten characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers
6.2.4 All administrator-level passwords shall be changed at least every 90 days
6.2.5 Where available, two-factor authentication shall be used to provide additional security
6.2.6 All users shall use uniquely named user accounts.
6.2.7 Generic user accounts that are used by more than one person or service shall not be used.

6.3 User Access

6.3.1 Access to information shall be based on the principle of “least privilege” and restricted to authorised users who have a business need to access the information.
6.3.2 Standard user accounts are assigned to authorised employees and should be used for work purposes.

6.4 Administrator-level access

6.4.1 Administrator-level access shall only be provided to individuals with a business need who have been authorised by Security Officer.
6.4.2 A list of individuals with administrator-level access shall be held by the Security Officer and shall be reviewed every 6 months.
6.4.3 Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.
6.4.4 To mitigate damage in the event of an attack, the use of Administrative Accounts is strictly limited to the execution of software making significant security-relevant changes to the operating system for some or all users and the creation of new accounts and allocation of their privileges.

6.5 Application Access

6.5.1 Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
6.5.2 Authorisation to use an application shall depend on a current licence from the supplier.

6.6 Hardware Access

6.6.1 Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only

6.7 System Perimeter access (firewalls)

6.7.1 The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.

6.7.2 All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.

6.7.3 The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly

6.7.4 All firewalls shall be configured to block all incoming connections.

6.7.5 If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

6.8 Monitoring System Access and Use

6.8.1 An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.

6.8.2 The business reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

7. Asset Management

7.1 Asset Ownership

7.1.1 Each information asset, (hardware, software, application, or data) shall have a named custodian who shall be responsible for the information security of that asset.

7.2 Asset Records and Management

7.2.1 An accurate record of business information assets, including source, ownership, modification and disposal shall be maintained.

7.2.2 All data shall be securely wiped from all hardware before disposal.

7.3 Asset Handling

7.3.3 Prochainmatrix shall identify particularly valuable or sensitive information assets through the use of data classification.

7.3.4 All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

7.3.5 All company information shall be categorised into one of the three categories in the table below based on the description and examples provided:

Table: Schedule 3.1: Categories for information classification. (ICP-P-0920-01)

Category	Description	Example
Public Information **(Green Information)**	Information which is not confidential and can be made available publicly through any channels.	• Details of products and services on the website • Published company information • Social media updates
Confidential **(Amber Information)**	Information which, if lost or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners	• Company operating procedures and policy • Client contact details • Company plans and financial information • Basic employee information including personal data
Sensitive **(Red Information)**	Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners. This information requires the highest levels of protection of confidentiality, integrity and availability.	• Client and company intellectual property • Data in information systems • Employee HR details • Any information defined as "sensitive personal data" under the Data Protection Act

7.4 Removable media

7.4.1 Prochainmatrix does not use removable media (such as USB memory sticks and recordable CDs/DVDs) to store business data.

7.4.2 Where indicated by the risk assessment, systems shall be prevented from using removable media.

7.4.3 Users breaching these requirements may be subject to disciplinary action.

7.5 Mobile working

7.5.1 Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements.

7.5.2 Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Security Officer.

7.5.3 Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.

7.5.4 Users must inform the Security Officer immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

7.6 Personal devices / Bring Your Own Device (BYOD)

7.6.1 Where necessary, staff may use personal mobile phones to access business email. This usage must be authorised by the Security Officer. The device must be registered in the asset records and must be configured to comply with the mobile working section and other relevant sections of this policy.

7.6.2 No other personal devices are to be used to access business information

7.7 Social Media

7.7.1 Social media may only be used for business purposes by using official business social media accounts with authorisation from Security Officer. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

7.7.2 Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.

7.7.3 Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company.

7.7.4 Users breaching this requirement may be subject to disciplinary action.

8. Physical and Environmental Management

8.1 In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.

8.2 Systems shall be protected from power loss by UPS if indicated by the risk assessment.

8.3 Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

9. Computer and Network Management

9.1 Operations Management

9.1.1 Management of computers and networks shall be controlled through standard documented procedures that have been authorised by Security Officer.

9.2 System Change Control

9.2.1 Changes to information systems, applications or networks shall be reviewed and approved by the Security Officer.

9.3 Accreditation

9.3.1 The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.

9.3.2 They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the Security Officer before they commence operation.

9.4 Software Management

9.4.1 All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
9.4.2 All software security updates/patches shall be installed within 7 days of their release.
9.4.3 Only software which has a valid business reason for its use shall be installed on devices used for business purposes
9.4.4 Users shall not install software or other active code on the devices containing business information without permission from Security Officer.
9.4.5 For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

9.5 Data Storage and Backup

9.5.1 As a Software as a Service provider, Prochainmatrix has developed an extensive source code on which the client services are based on.
9.5.2 Backup plans apply to the Prochainmatrix source code, client applications and client data stored in SQL databases.
9.5.3 Backup copies of data are protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.
9.5.4 Prochainmatrix uses the cloud providers Microsoft OneDrive through Redcentric and GoDaddy.
9.5.5 Corporate data shall be stored on the company shared drive and not to be stored on the local machine/s, and backups are carried out on regular intervals.
9.5.6 Prochainmatrix has a service-level agreement with Redcentric who is responsible for scheduling and completing backups between 8pm and 4pm to avoid client interaction.
9.5.7 The data is stored away from the deployed virtual machines, therefore on Redcentric assets.
9.5.8 Deployed virtual machines are part of a formal order, instructing Redcentric to make them available as and when they are needed.
9.5.9 Every virtual machine is installed with a backup client and backups are executed automatically based on a server schedule and data stored for 30 days.
9.5.10 The process generates logs which are monitored by Prochainmatrix to ensure incidents can be logged and investigated as soon as possible so that remedial action can be agreed with Redcentric.

9.6 External Cloud Services

9.6.1 Where data storage, applications or other services are provided by another business (e.g. a ‘cloud provider’) there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

9.7 Protection from Malicious Software

9.7.1 The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
9.7.2 All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device’s operating system

9.7.3 All anti-malware software shall be set to scan files and data on the device on a daily basis, scan files on-access, automatically check for, and install, virus definitions and updates to the software itself daily, and block access to malicious websites.

9.8 Vulnerability scanning

9.8.1 The business shall have a yearly vulnerability scan of all external IP addresses carried out by a suitable external company.
9.8.2 The business shall act on the recommendations of the external company following the vulnerability scan to reduce the security risk presented by any significant vulnerabilities
9.8.3 The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

10. Response

10.1 Business Continuity and Disaster Recovery Plans

10.1.1 The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
10.1.2 The Information Security Officer shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

10.2 Breach Reporting Process

10.2.1 In the event of a breach, incidents shall be reported to the Security Officer and Prochainmatrix’s Security Incident Log will document the facts as they are uncovered; including an incident timeline, assets affected, subjects involved, and rectifying actions taken.
10.2.2 If deemed necessary by the Security Officer, data will be isolated to facilitate forensic examination.
Security and data breaches will be formally reported to the ICO without undue delay and within 72 hours.
10.2.3 Prochainmatrix will take actions to immediately contain the breach and carry out an risk assessment led by the Security Officer.
10.2.4 We will ensure individuals are directly notified about personal data breaches without delay via email with a follow up call and advised on how to protect themselves from any effects of the breach.
10.2.5 The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

11. Further Information

11.1 Further information and guidance on this policy can be obtained at governance@prochainmatrix.co.uk