Information Security Policy

1. Amendment History

Issue	Date Issued	Reason for Change	Ref Authority
0.1	18/3/18	Initial version	LP/TP
1.0	29/03/18	Released	MR

2. Contents Page

3. Objectives

The Information Security Policy objective is designed to:

- Protect company and customer from unauthorised access.
- Deliver a compliant and enabling environment that balances Information Security with appropriate accessibility and provides the optimum level of risk management to support the achievement of Datel Protex Systems Limited’s strategic goals.
- Ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure that users are aware of and comply with all current and relevant EU and UK legislation.
- Responding to changes in the context of the company as appropriate, initiating a cycle of continuous improvement.

The three main principles of this document are:

- **Confidentiality**

  Information is protected and accessible to only those who require access to efficiently perform their role.

- **Integrity**

  Safeguarding the accuracy and completeness of data, processing methods and reports.

- **Availability**

  Data is available to authorised personnel when required.

Compliance of this policy will also ensure that all legal, regulatory and contractual obligations are met.

4. Scope

The Information Security Policy covers storage, access, transfer and destruction of information during the course of business. Therefore, it applies to the conduct of staff and third-party contractors with authorised access to that information, as well as the applications, systems, equipment and premises that create, process, transmit, host or store information, whether in-house, personally owned, provided by customers, third party contractors or suppliers.

5. Accountabilities

The Information Security Officer is the accountable owner of the Information Security Policy and its maintenance and review.

The Information Security Officer is responsible for compliance, investigating actual, potential or suspected breaches of this policy. Breaches of information security controls must be reported to the Information Security Officer by the appropriate department head where a breach has been reported. Actual, potential or suspected breaches will be reported to the Executive team monthly.

6. Review

This policy, and its subsidiaries, shall be reviewed and updated regularly to ensure they remain appropriate. Additional policies may be created to cover specific areas.

7. Policy

The objectives will be achieved by the guidance outlined in this document as follows.

7.1. Access Control

Objective: To limit access to information and information processing facilities.

7.1.1. Access to networks and network services

- All users are to be allocated roles to determine the level of access granted. Security Groups are used with the Group policy defined in the Active Directory for the domain.
- Security Groups are to be reviewed annually to ensure correct permissions are given to all users.
- Individual user accounts with unique identifiers are to be used for all users.
- Employees are forced to change their domain passwords at first log-on.
- Password to networks are not to be reused.
- All user passwords are to comply with the Datel Password Policy. The password policy enforces passwords meet minimum requirements and are changed regularly.
- Employees or external party users must not write down or store passwords in plain text. All users are expected to keep their user IDs and passwords secure and never disclose to any persons either internal or external.
- Systems and applications are to log unsuccessful and successful logon attempts with failed login attempts reviewed and appropriate actions taken.
- Logons to company resources should not transmit passwords in clear text over a network.
- Inactive remote access sessions are to be terminated within a period of inactivity.

7.1.2. Access management

- Users are only to be granted access to the minimum level of resources and services that they require in order to fulfil their duties.

- The access rights of all employees and external third-party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
- Redundant user IDs are not to be assigned to other users.
- When a user leaves the Company, their user ID is to be immediately disabled from logging in to access resources. When the ID is no longer required, it us to be removed.
- User access controls are reviewed periodically and at least annually to ensure that redundant users cannot be used to access resources. If a redundant ID is no longer required, it should be removed.
- A user is not to be granted access to resources until authorisation procedures have been completed.
- If an employee changes role within the company, their access rights are to be reviewed to ensure that they have the appropriate access.

7.1.3. User Responsibilities

- Users are instructed to keep passwords confidential and ensure that it is not divulged to any other parties including people of authority.
- Users are instructed to avoid keeping a record on paper, software or handheld device any passwords unless this can be stored securely, and the method of storing has been approved by the company.
- Users are instructed to change passwords whenever there is any indication of a compromise to this information.
- Users should select quality passwords that are easy to remember but not based on information related to themselves that can be easily guessed. Passwords should also not consist of words vulnerable to dictionary attacks and should be free of consecutive identical all numeric or all alphabetic characters.
- Not use the same password for company and non-company related activities.
- Ensure that when logging onto company resources, passwords cannot be compromised. Users should ensure that no other person can witness their logging onto company or customer resources.
- If a user suspects that the device being used to logon to either company or customer resources has been compromised, they are to report this potential breach to their manager.

- All users must adhere to the acceptable use policy.
- Automatic access locking is to be implemented where available. Where automatic access locking is not available, users must ensure that they terminate active sessions when finished. Users must also log-off from applications or network services when no longer needed.

7.1.4. Access to customer and third-party networks

- Customers are to provide Datel with a unique log-in with a strong password for the company to access their network.
- Customer login and password information that is to be used by Datel is not to be provided to third parties either by the customer or by the company employees.
- Where WebEx is used to dial onto customer machines, WebEx recordings are not permitted unless authorised by a Director. Each user is required to have their own WebEx user id and password. Passwords are to conform to WebEx's password policy.
- Screen recording whilst remotely connected to customer systems is not permitted unless authorised by a Director.

7.1.5. Remote network access

- Remote access to network services is provided to employees by a secure VPN. No other method of access to company network services is to be used unless written permission is given by a company Director.
- Only individually named users can be used to access the company network remotely. Generic accounts must not be used to access company network resources.

7.1.6. Access to PCs and laptops

- Local administrative rights are not assigned to employees ensuring users cannot install unapproved software. Only authorised users have local admin rights to their own PCs and laptops. If local administrative rights are required, this can be requested through Internal IT who will use the Local Admin Password Solution (LAPS).
- Administrative accounts are to be individually named users and not generic accounts.
- Only PC's and laptops provided by Datel Protex Systems Limited to be used to Datel or customer networks. Therefore, no home PC's or personal laptops should be used, unless authorised by a Director.

- All unattended laptops are locked. Laptops are to be taken home where practical as per the Business Continuity Plan.

- All laptop screens are to be locked when not in use.

7.1.7. Clear desk and clear screen policy

- Personal data or critical business information that is either owned by the company or has been entrusted to the company, whether printed on paper or stored on electronic storage media, must be locked away in either a storage cabinet or other forms of security furniture when not required especially when the area in which the information is held is vacated.

- Computers or terminals that are not-removed temporarily should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password or token.

- Unauthorised use of photocopiers and other reproduction technology for copying customer data or personal information is prohibited.

- Media containing personal or classified information should be removed from printers immediately.

7.2. Application Security

Objective: To ensure that applications used by the company that access personal or classified information are protected from unauthorised change.

7.2.1. Company application security

- Applications that are required to access personal or confidential information are either installed in secure environments with restricted access or do not store clear text passwords in unencrypted files or database objects.
- For those applications that utilise databases, those databases must have secure access such that only authorised employees can access the data outside of the application.
- Changes to company applications that hold personal or confidential information, including changes to software, configuration and security mechanisms are controlled via a change management process.
- All application servers that contain personal or classified information and also those servers that provide access to company resources are to be time synchronised to ensure that internal monitoring and security access can be traced to a single time source.

7.2.2. Customer application security

- Where SQL Server is installed by Datel Protex Systems Ltd staff, we advise the SA password to be changed following installation and that a Datel administrator password for SQL Server is created and enabled when required and disabled when not needed.
- For Windows Authenticated accounts used to run services required by Datel installed software, the customer will be asked to provide a password that conforms to their password policy or will be provided with a unique password.

7.2.3. Instant Messaging (IM)

- Only Company approved instant messaging applications are to be used to share business related information.
- Only IM applications that provide secure messaging capability will be approved.
- When approving IM applications, the company should consider only those applications where user accounts can be company created user accounts and can be suspended upon termination of employment.
- If a customer requests communication via an unapproved IM application, the employee must obtain approval from their manager or a Director and if approved, the IM application should be added to the approved software register.

- Employees using IM to communicate business related information should use company provided equipment or equipment approved for company use. Only business user accounts can be used to communicate business related information via IM, the use of personal accounts is prohibited.

7.3. Mobile Devices

Objective: To ensure the security of mobile devices.

- All users receiving mobile devices that are to be used for the access of business information are required to have signed an end user agreement acknowledging their duties, waiving ownership of business data, allowing remote wiping of data by the organisation in case of theft or loss of the device or when no longer authorised to use the service.

- Company equipment that contains classified information such as Laptops, iPads and iPhones must be remotely wiped in the event an item is lost or stolen.

- iPhone and iPad’s must to be password protected and biometric restrictions turned on.

7.4. Remote Workers

Objective: To ensure the security of remote workers.

- The physical security of a remote workers location will be reviewed when first employed to ensure that the location does not provide unsecured access to personal or classified data
- The employee will provide details of their remote access to the Company to ensure that access is not obtained over unsecure networks.
- Employees are not permitted to provide access to Company resources, nor provide Company information or information relating to customers of the Company to family or visitors.
- Remote employees are only permitted to access Company resources and data via equipment provided by the Company.
- Remote workers are not permitted to install unapproved software onto Company equipment.
- Employees are required to ensure that Company property and Company information is kept in a secure location within the employee working location.
- Employees are not permitted to prevent the Company from auditing Company property for installed software and security configurations.
- Employees are only permitted to backup Company information to approved storage locations and devices.
- When remote worker employment with the Company is terminated, employees are required to return all company equipment to the Company and remote access to Company network and resources are disabled.

7.5. Human Resource Security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are being considered.

7.5.1. Screening of Employees

To ensure that background checks on all candidates are carried out in accordance with the relevant laws, regulations and ethics and are proportional to business requirements, the classification of information to be accessed and the perceived risks.

- One business and one personal character reference are to be obtained prior to commencement of employment.
- The candidate's CV is to be verified for completeness and accuracy
- The candidate is to provide a valid photographic identification to verify the candidate's identity prior to the commencement of employment.

7.6. Asset Management

Objective: To identify organisational assets and define appropriate protection.

7.6.1. Purchase of assets

- Any device purchased for use by employees or third-party users should be inspected upon receipt for evidence of tampering. If tampering is discovered, it should be reported immediately to a manager or Director.

- Where devices are received with preloaded software, the device should be examined using the company approved software for identifying virus or malicious software. If a virus or malicious software is discovered, it should be reported immediately to a manager or Director.

- A register of fixed assets is maintained by Internal IT and includes laptops, iPhones, iPads and external hard drives.

7.6.2. Location of Assets

- Any device that provides access to personal or confidential information should be positioned to minimise unnecessary access or visibility of confidential information.

- Devices that provide access to company resources or personal or confidential information should not be positioned in locations that can be accessed without key cards. Such devices should not be located in areas where unauthorised staff are able to access such areas.

- An asset can only be removed to a permanent off-site location when authorised by a Director and the asset along with its new location is to be recorded in the asset register. Returning assets must be inspected for tampering, virus infected or malicious software.

- Assets holding personal or confidential information may not be taken to a location outside the EAA.

7.6.3. Return of assets

- All employees and external users should return all organisational assets (physical or electronic), in their possession upon termination of their employment, contract or agreement.

- In cases where an employee or external party user purchases the organisation’s equipment or uses their own personal equipment, all electronic assets owned by the

Company or entrusted to the Company are to be transferred to the Company and erased from the equipment.

- In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the Company.
- During the notice period of termination, the employee or external party user is prohibited from copying electronic assets owned or entrusted to the Company unless permission is granted by a Manager or Director of the Company.

7.6.4. Disposal of assets

- All items of equipment containing storage media is to be verified to ensure that any personal or confidential data and licensed software has been removed or securely overwritten prior to disposal or reuse.
- Items are to be verified to ensure whether or not storage media is contained prior to disposal or reuse.
- Storage media containing confidential or copyrighted information is to be physically destroyed or the information is to be destroyed, deleted or overwritten to make the information non-retrievable. Standard delete or formatting is not to be carried out.
- Damaged equipment containing storage must be risk assessed to determine whether the media should be physically destroyed or sent for repair, or discarded.
- Where storage media is to be repurposed, the media is to be encrypted prior to re-use.

7.6.5. Removable Media

- If no longer required, the contents of any reusable media that are to be removed from the Company should be made unrecoverable and the asset register updated to reflect the removal of the reusable media.
- All removable media that contains electronic assets owned by or entrusted to the Company should be stored safely and securely when not in use.
- All removable media that contains electronic assets owned by or entrusted to the Company should be encrypted to protect the data.
- Removable media is only to be used if there is a business case for doing so. Employees requiring removable media must obtain their manager's permission before requesting removable media.

- All removable media obtained by employees must be recorded in the asset register and must be clearly identifiable.
- The removable media is only to be used for the purpose it was requested.
- If no longer required, removable media containing electronic assets owned by or entrusted to the Company are to be stored and disposed of securely. Disposal of the removable media is to be recorded on the asset register.

7.6.6. Customer Information

- Access to Customer assets will only be granted to those employees that require access.
- Customer shared data will not be shared with third parties without written consent from the Customer, where applicable, Datel may request third parties to contact the Customer directly for access to data.
- Non-disclosure agreements (NDA's) are to be strictly adhered to. Where an NDA is requested, all members of staff are notified. The NDA should clearly define the areas protected by the agreement.
- NDA's can only be agreed by a Director of the company.
- All Customer shared data will be logged within the Customer Data Register in accordance with the Customer Data Register procedure.
- Every time customer shared data is moved or copied to another location, a new entry in the Customer Data Register must be authorised and logged separately.
- No customer information is to be stored on employee devices once the need for this information has passed (such as the completion of a project or support ticket), or once the time limit for the use of this data has expired if such a time limit has been agreed. This information must be removed securely from the device.
- Customer data stored by Datel, either in Datel data centres or employee equipment, should not be used for any purpose other than those stipulated in the Data Register and agreed in writing by the customer.

7.6.7. Information Sharing

- Personal or confidential information must not be shared to anyone without prior approval from the information owner or a manager or Director of the company.
- Where personal or confidential information is to be shared, only approved sharing mechanisms must be used.

- Information is shared with Customers via the Datel Portal. Where personal or confidential information such as data extracts is to be provided to Datel by the Customer, this can be sent via the authorised secure upload facility.

- Personal or confidential information such as user IDs, passwords or customer data should not be shared by email unless approved by a manager or Director, and an approved email encryption is used.

- If confidential information is to be communicated verbally over the phone, employees must ensure that they are in a location that cannot be overheard by anyone that is not approved to hear such information.

- If a facsimile is to be used to receive confidential information, employees must ensure that the receiving facsimile machine is manned by authorised personnel and that the machine is not left unattended.

- If confidential information is to be posted, employees must ensure that the information is sealed and sent via an approved courier.

7.7. Physical and Environmental Security

Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities and to prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

- The offices are alarmed and maintains CCTV surveillance. A key card is required to gain entrance to the main offices beyond reception, which has restricted access to areas such as server and stock rooms.
- Reception areas are manned during the hours of 8am and 5.30pm after which the main entrance is secured by key card access only. All other entrances are secured by Key Card access only.
- Access permissions to secure areas are reviewed regularly.
- Visitors are to sign into and out of the building, confirm who they are visiting and their car registration details.
- Visitors are not permitted to be left unsupervised in areas that contain confidential or personal information or in areas that have unsecure access to other areas that contain confidential or personal information.
- A clear desk policy of confidential information and removable storage media is in place.
- Risk assessments are conducted on the building at regular intervals.
- Wireless networks are separated between corporate and guest access. Guest wireless networks are restricted to non-Datel network access and a password is required.
- Access to corporate wireless network is restricted to domain user accounts.
- Where a non-authorised employee or third party is required to access a secured area, they are to be accompanied by an authorised employee and are to have access granted by a manager or Director responsible for the secured area. Any third party requiring access to a secure area is to have their access recorded.
- Unsupervised working in secure areas is not permitted.
- Photographic, video or other recording equipment such as cameras or mobile devices are not allowed in secured areas unless authorised.
- Access to any area in the building that contains devices or equipment that has access to confidential or personal information should be accessed via at least one internal security access mechanism after point of entry.

7.8. Operations Security

Objective: To ensure that information and information processing facilities are protected against malware, protect against loss of data, record events and generate evidence, ensure the integrity of operational systems and to prevent exploitation of technical vulnerabilities.

- Anti-virus to be installed on all laptops, virtual machines and servers, which are regularly updated in-line with the OP9 Internal IT policy.
- Backups are managed in line with OP9 Internal IT and OP9C - Internal IT - Server, Network, VPN Support policies.
- Datel Advansys Limited manage the infrastructure of Datel Protex Systems Limited. Monthly reporting includes, but not limited to: backup success status, server health and security incidents, as described in OP9C - Internal IT - Server, Network, VPN Support
- Employees are prevented from the use of known or suspected malicious websites.
- Emails and attachments are scanned for malware before use.
- All servers which store confidential or personal data are updated with security updates as per the Datel Security Update policy.
- iPhones and iPads are to be updated to the latest version within 28 days from their general availability.
- Only approved software detailed in the Register of Approved Software can be loaded onto laptops. Employees advised on the risks of obtaining files and software from or via external networks, or via any other medium and on what protective measures should be taken. Use of unapproved software must be investigated.
- Software used by the company is acquired through known and reputable sources. Proof of ownership and locations as to where software is installed is registered on the software asset register. Assets are reviewed periodically to ensure that only approved and licensed software is installed.
- Every department has a standard computer build profile that describes the configuration and software to be installed.

7.9. Encryption

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

- All laptop internal drives to be encrypted.
- All external hard drives to be encrypted.
- Recovery keys are not to be written down, saved to unsecure devices, printed or disclosed. Only network administrators should have access to recovery keys.
- Only authorised cryptographic security systems are to be used to protect company information.
- Connection to customer systems should be via encrypted connection.

7.10. Compliancy

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements and to ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

- Establish responsibility and accountability for Information Security within Datel Protex Systems Limited.
- Management and staff to maintain an appropriate level of awareness, knowledge and skill to minimise the occurrence and severity of Information Security incidents.
- New employees are required to read, understand and sign the Security Policy. Security training will be carried out as part of the Quality Workshop for new employees.
- Periodic information security training to be undertaken by employees.
- All applicable legislative and contractual requirements to be followed as per Datel Protex Systems Limited's policies and procedures.
- Only licenced and approved software to be installed and used. PC's and laptops will be monitored regularly for unauthorised software.
- Periodic audits and policy reviews to ensure full compliance legislation and the adoption of the policies, as detailed in the audit plan. All documentation of audits to be retained for a minimum of 7 years.

7.11. Third Party Relationships

Objective: To ensure protection of the organisations assets that is accessible by third parties and to maintain an agreed level of information security and service delivery in line with supplier agreements.

- Third party contractors and suppliers, where accessing company resources and information must understand and comply with the Information Security policy and sign an agreement to confirm acceptance of the policy and a non-disclosure agreement.

- Access to networks and information systems by third-parties is restricted to only areas that are required.

- Each third-party user that requires access to company network and information must be provided with unique IDs and are also required to create a password to conform with company password policy.

- Where customer data is required by the third-party in order to carry out tasks sub-contracted by the company to the third party (such as copies of customer data), this data is to be obtained by the third party by the customer directly.

- Where a third party requires access to customer networking or systems and the third party is contracted by the company, an authorised company representative is to request that the customer contacts the third party directly to arrange for access to network and systems and that the credentials provided to the third party are unique and are not those used by the company employees.

- If a third-party user (such as a contractor), is acting on behalf of the company and that the third-party company has no relationship as such with the customer outside of the relationship via the company, the third-party user is to be treated as a member of the company and therefore is required to read and confirm acceptance of this security policy. Suspected breach of this policy by third party users when accessing customer resources will result in the suspension of the third-party users access permissions until investigated further by a representative of the company.

- Third-party users are not permitted to share either network/application access information, or confidential data provided by the company without explicit permission from the company.

7.12. Security in Development Processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

- Source Code is not to be shared with third parties without agreement from a Datel Director. An NDA is required to be signed both by the receiving party and a Datel Director.
- Source Code received from third parties needs to be agreed by a Datel Director and investigated for malicious coding, prior to being used.
- A register of approved third-party libraries to be maintained, to ensure coding is obtained from authorised libraries to protect against malicious coding and any licencing constraints.
- Open Source libraries or code need to be added to the release information and any licencing implications considered.
- SSL certificates are to be purchased from a reputable source for use in both development and systems implementation. Where software is being implemented on a customer server, the customer is required to purchase the SSL certificates from a reputable source.
- Access to source code and associated items such as designs, and specifications are to be strictly controlled in order to prevent the introduction of unauthorised functionality and to avoid unintentional changes. Only users that require access to specific areas of source control and other development artefacts are to be granted access to such source code and artefacts.
- Source code is not to be deployed to operational systems.
- Source code is not to be accessed across unsecured networks.
- Test data must be selected carefully and controlled. Where the test data is of a confidential nature (for example, contains real financial information or customer details), access to the test data and systems that can access the test data must be restricted to authorised employees only.
- Customer test data should be removed from company assets when testing is complete.

7.13. Information Security Continuity

Objective: Information security continuity shall be embedded in the organisation’s business continuity management systems.

- Ensure the organisation can continue its commercial activities in the event of a significant Information Security incident.
- Periodic reviews and testing of the Business Continuity Plan to be undertaken and documented.

7.14. Management of Information Security Incidents and Improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

- Security incidents should be reported to a Manager or Director within timescales dictated in the security incident procedure. The Manager or Director will be responsible for initiating the security incident procedure and all security incidents are to be documented in the Security Incident Log.
- Root cause analysis of the security incident will be carried out as per the security incident procedure.
- A culture of continual improvement is encouraged to maintain high security standards across the business.
- Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services