

INFORMATION SECURITY POLICY

PRAGMATIC SOLUTIONS

Version:	2.6
Date of version:	October 2025
Created by:	Compliance Team
Approved by:	Lloyd Lemmon
Confidentiality level:	Internal

Table of Contents

<i>Introduction.....</i>	3
<i>1. Organization of information security.....</i>	4
<i>2. Teams and Responsibilities.....</i>	4
2.1. Teams contact details	6
<i>3. Asset management.....</i>	6
<i>4. Human resources security.....</i>	6
<i>5. Physical & environmental security.....</i>	8
<i>6. Communications & operations management</i>	8
<i>7. Access control</i>	10
<i>8. Information systems acquisition, development & maintenance</i>	14
<i>9. Information security incident management</i>	16
<i>10. Business continuity management.....</i>	16
<i>11. Compliance.....</i>	17
<i>12. Virtual Private Network (VPN) Policy</i>	18
<i>13. Desktop and Laptop Computer Security.....</i>	19
<i>14. Media and Equipment Disposal.....</i>	23
<i>15. Removable Media Policy</i>	26
<i>16. Encryption Key Protection Policy.....</i>	27
<i>17. Password Management</i>	29
<i>18. Data Classification</i>	29
<i>19. Breaches of Policy.....</i>	31
<i>20. Revision and update of present policy</i>	31
<i>VERSION HISTORY.....</i>	31

Introduction

Purpose

It is Pragmatic Solutions intent to fully protect the confidentiality, integrity and availability of all its business information to safeguard the company's assets, customers, staff and reputation.

This Policy has been created as part of an internal and operational control and process for the use of the company's information technology (IT) tools including but not limited to computers, personal digital assistants (PDA) such as smart phones, tablets, email, software, telephone, internet use as well as outlining the consequence of misuse. This policy will outline what is expected of the user by the company.

This information security policy has been based on the international standards ISO/IEC 27001 (Information technology - Security techniques - Code of practice for information security management).

All employees, contractors, vendors and third parties that use, maintain or handle Pragmatic Solutions information assets must follow this policy. Policy exemptions will be permitted only if approved in advance and in writing.

The objectives of this policy are:

- To protect Pragmatic Solutions business and customer information from unauthorized disclosure, modification or loss.
- To establish safeguards to protect Pragmatic Solutions information resources from theft, abuse, misuse and any form of damage.
- To establish responsibility and accountability for information security.
- To ensure that Pragmatic Solutions can continue business in the event of significant information security incidents.
- To ensure Pragmatic Solutions compliance with applicable laws and regulations and industry best practice.
- To encourage management and employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of information security incidents.

Structure of procedures within this policy

Pragmatic Solutions' policies and procedures are structured into categories. This document mentions most of the below procedures, in terms of information

security and ISO 27001. Within the categories there are standalone documents which are focused on particularly critical or in-depth areas of Pragmatic Solutions business.

This document contains a summary of our policies and guidelines for procedures in place for each of these areas.

Each area contains the specific information security measures even though specific policies and procedures exist for specific areas.

1. Organization of information security

Policy objective

Provide guidelines for how the Information Security Team (IST) effectively should manage information security within the Pragmatic Solutions organization scope. The IST may delegate some or all the policy sections but is ultimately responsible for its implementation.

Procedure guidelines

- The Pragmatic Solutions' management team should meet at least once a year to review the status of Pragmatic Solutions' information security, approve new or modified security policies and other high-level security management activities.
- A list of contacts is maintained for authorities such as law enforcement, money laundering and regulatory bodies, emergency services, health & safety and services providers (power, water, cooling etc.).
- Contact with third party companies shall be maintained and confirm that special interest groups or other specialist security forums and professional associations assist in the protection of the gaming setup.
- The Head of Legal and Compliance must ensure that all contracts and agreements with 3rd parties comply with Pragmatic Solutions' security policies and include appropriate Non-Disclosure Agreements (NDA's).
- A set of information security policies, of which this document is one, should be written, agreed and communicated to all employees and 3rd party organizations so that security requirements and obligations are well understood by all concerned.

2. Teams and Responsibilities

Different groups are required to maintain company security. Employees, teams, and departments involved in security maintenance, are conventionally called the IST (Information Security Team). The groups:

- IT team
- Tech Support team
- Release team
- QA team
- Management
- Finance
- HR

Tech Support team

They are the first team that will need to act in the event of an incident. Tech Support team is responsible for monitoring all environments.

IT and DevOps team

IT Team oversees the entire production infrastructure and configuration. This team is responsible for regular deployments, patch management and for providing specific monitoring tools.

Release team

The Release Team will be responsible for ensuring that all enterprise applications operate as required to meet business objectives on a regular basis. They are primarily responsible for ensuring and validating appropriate application performance and may assist other Security Teams as required.

QA team

QA team is responsible for testing and quality assurance of all enterprise applications.

Management team

The Management Team will make any business and financial decisions for the day-to-day operations. Decisions that will impact the company are made by this team, as well as aspects related to company information security. The IST will ultimately report to this team.

Finance team

This team will be responsible for ensuring that all of finance needs are dealt with in an appropriate and timely manner on an ongoing basis. The finance team will ensure that there is money available for expenses for day-to-day business functions.

HR team

This team will be responsible for ensuring that all employees/consultants are informed and educated about Pragmatic Solutions' information security policies and acceptable use guidance.

2.1. Teams contact details

Team	Member	Contact details
CTO	Ravi Auchuri	E-mail: ravi@pragmatic.solutions
Technical support		E-mail: technicalsupport@pragmatic.solutions Skype: live:.cid.af5357ed6e5c03e4
Management	Ashley Lang Peter Mares	E-mail: ashley@pragmatic.solutions E-mail: peter@pragmatic.solutions
Finance & HR	Flavia Georgescu	E-mail: flavia@pragmatic.solutions

3. Asset management

Policy objective

Ensure Pragmatic Solutions information systems and assets are tracked and maintained in accordance with their sensitivity and criticality.

Procedure guidelines

- Usage of all Pragmatic Solutions internal office software assets (licenses and possibly media), including internally developed software, must be tracked in an inventory.
- Possession or usage of unlicensed software on any Pragmatic Solutions information systems is strictly prohibited.
- Pragmatic Solutions has legal ownership of all files and messages stored or transmitted on its computer and network systems and reserve the right to access this information without prior notice.

4. Human resources security

Policy objective

Ensure that employees, contractors and 3rd parties are suitable for their roles and understand their security responsibilities, and to reduce the risk of theft, fraud and misuse of facilities. This applies to all employees, contractors and 3rd party companies working on behalf of Pragmatic Solutions.

Procedure guidelines

- Prospective employees, contractors and 3rd parties must be screened in line with relevant laws and background checks should be performed before any offer of employment or contract is made.
- Security roles and responsibilities must be a part of all employment and 3rd party contracts and these must be signed by employees or contractors before commencing the engagement.
- All employees should be given regular security awareness training appropriate for their role and made aware of security policies which are applicable to them.
- A formal disciplinary process should be established for employees who have committed a security breach.
- Responsibilities and procedures for employment termination, such as return of any company assets and removal of access rights or account deletion must be written and assigned.
- Employee access to Pragmatic Solutions' systems and applications will be tracked and monitored. Accounts and access will be removed upon termination of employment.
- All documents the employees give Pragmatic Solutions will be treated as confidential and can only be accessed by staff in relevant positions.

Termination Policies

Written termination policies are established to provide clearly defined steps for employee separation. It is important that policies are structured to provide adequate protection for the organization's computers, assets and data. Termination practices address voluntary and involuntary (e.g., immediate) terminations. For certain situations, such as involuntary terminations under adverse conditions, the company has clearly defined and documented procedures for escorting the terminated employee from the premises. In all cases, however, the following control procedures should be applied:

- Return of all access keys, ID cards and badges-to prevent easy physical access
- Deletion/revocation of assigned login IDs and passwords - to prohibit system access

- Notification to appropriate staff and security personnel regarding the employee's status change to "terminated"
- Arrangement of the final pay routines - to remove the employee from active payroll files
- Performance of a termination interview - to gather insight on the employee's perception of management
- Return of all company property

5. Physical & environmental security

Policy objective

Prevent unauthorized physical access, damage and interference to Pragmatic Solutions' premises and information assets. All buildings and facilities rented or operated by Pragmatic Solutions.

Procedure guidelines

- Buildings and equipment must be protected against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disasters (servers held at co- location).
- All critical production and office environment equipment must be protected and maintained:
 - Power failure protection (UPS)
 - Heating, ventilation and air-conditioning (HVAC) provision and failure protection
 - Cable duct protection for power and telecoms lines
- All equipment must be correctly operated and maintained to ensure its continued availability and integrity of maintenance and support agreements.
- Equipment containing any form of media storage must be securely disposed of at end-of-life.
- Equipment must not be taken off-site without prior authorization.

6. Communications & operations management

Policy objective

Ensure the correct and secure operation of all Pragmatic Solutions information processing facilities.

Procedure guidelines

- Operating procedures should be documented, maintained and made available to all users who need them.
- As far as practical, duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or accidental modification or misuse of Pragmatic Solutions assets.
- All 3rd party service definitions and delivery levels (service level agreements or SLA's) should be included in the legal contracts and agreements and monitored for compliance.
- All information must be verified as correct from more than a single source at initial take-on and whenever subsequently changed.
- Acceptance criteria for all systems should be established and suitable tests of the systems carried out during development.

Backup

- All production server systems must be regularly backed-up using a standard backup methodology and backup media must regularly be transferred and stored off-site.
- Sensitive data must be encrypted both on disk and on the backup media and be capable of authorized decryption for at least as long as it is required for regulatory compliance.
- Backup systems must be periodically tested with a restore operation to ensure that the procedure works as expected.
- Backup media must be archived for the minimum period for regulatory compliance.

Operational procedures

- System and application logging must be enabled, and log files must be protected from deletion, modification or unauthorized access where possible. The production application should only have read / write access to the log files (no delete) and DBA's should only have read access (no write / delete).
- Log files must be periodically reviewed by the Technical team and any unusual activity alerted.
- The production CRM database must be used to generate daily exception reports of unusual customer activity. These reports must be reviewed daily by technical team.
- The principal of "least privilege" should be used for all privileged users (i.e. Administrator / Operator / DBA should only have sufficient privilege to perform their daily work).
- All privileged accounts must be identifiable and accountable to an individual.
- Full-privilege accounts should be created for controlled use (i.e. credentials stored in a safe). These accounts are for use in exceptional or unforeseen circumstances and their use must be authorized.
- All software and hardware faults must be logged and reviewed on a regular basis by the Technical team.

- All clocks in the production environment must be synchronized to an accurate time source to enable log file cross-referencing.
- Detailed production system documentation, such as designs, diagrams and specifications, must be marked and treated as Pragmatic Solutions Proprietary and protected against unauthorized access.

7. Access control

Availability, confidentiality and integrity are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital for the protection of systems and information authorized users who have access to Pragmatic Solutions systems and information are aware of and understand how their actions may affect security.

Availability – systems and information are physically secure and will be accessible to authorized persons when required.

Confidentiality – systems and information will only be accessible to authorized persons.

Integrity – the accuracy and completeness of systems and information are safeguarded.

Policy objective

Control access to Pragmatic Solutions information, systems and applications within the infrastructure.

Purpose

The purpose of this policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

Scope

The scope of this policy includes all access to Pragmatic Solutions information, ICT systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/creation, through to utilization, storage and disposal.

Responsibilities

Directors are responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems. Designated owners of systems, who have responsibility for the management of ICT systems and inherent information, need to ensure that staff have been made aware of their responsibilities toward security. Designated owners of systems and information need to ensure they uphold the security policies and procedures.

Procedure guidelines

- There must be a formal employee / contractor ("User") registration and deregistration procedure in place or granting and revoking access to all information systems and services within Pragmatic Solutions.
- Access to systems and applications is restricted to a username and password.
- All users should be given a unique user identifier, preferably common across all systems if access to multiple systems is required.
- It must be possible to track the access rights and privileges granted to individual users. These access rights and privileges should be reviewed periodically.
- Generic accounts must only be used when there is demonstrably no alternative, and all generic accounts used should be recorded, together with a list of individuals who have access to the generic accounts.
- All user passwords must be changed periodically (every 60 days) and be composed by a minimum of 12 characters. It should contain a mix of capital and lower-case letters and at least two characters must be numeric or a symbol/punctuation character. This policy must be enforced where possible at the Operating System level.
- All production systems must be configured with strong access controls and there must not be any vendor-supplied defaults in the production environment.
- The production application must strongly authenticate to the production database in a way that cannot also be used for unauthorized interactive access.
- The production application authentication to the production application must not use the same credentials that are also used elsewhere (i.e. in any test or staging environment).

Login considerations:

- All systems should be accessed by secure authentication of user validation. As a minimum, this should entail use of a Username and a Password.
- Login to systems/information should only be attempted using authorized and correctly configured equipment in accordance with Pragmatic Solutions policies.
- After successful logon users should ensure that equipment is not left unattended and active sessions are terminated or locked as necessary. Systems should be logged off, closed or terminated as soon as possible.
- System login data should not be copied, shared or written down.

Physical access and controls

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data:

1. Staff should wear their Pragmatic Solutions ID badges and visitors must wear the Visitor ID badges which have been issued to them. People who are not displaying ID badges should be challenged. Any person not known to location personnel must be challenged to establish who they are and whether authorization has been provided for them to be there. If there is any doubt about the identity of the individual, the appropriate security officer/manager should be contacted to confirm the individual's identity. Staff in residential establishments will need to check their local procedures whilst working inside the home.
2. Appropriate recording mechanisms need to be in place to record the names, dates, times and signatures for the signing in and out of visitors (including Pragmatic Solutions' personnel) to Pragmatic Solutions locations. All visitors must be issued with an authorized Pragmatic Solutions visitors badge when signing in.
3. The use of keys to buildings, rooms, secure cabinets, safes etc. must be controlled and recorded. Keys must be stored in secure areas/locked cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be always known and a signing in/out recording mechanism must be maintained to record the serial/ID of keys against individual names when keys are used.
4. Electronic access fobs must be issued to authorized staff on an individual basis. Staff issued with access fobs must have their names and employee numbers recorded against the registered access fob number including date and time of issue
5. Access fobs should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorized personnel may be permitted to use another authorized person's fob if available with permission of the line manager and the recorded user must either be present or be made aware that their fob is being used. Any such use must be recorded and maintained in a logging system for this type of event
6. Access fobs issued to personnel who no longer work for the Pragmatic Solutions must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system.
7. Locations housing critical or sensitive information and/or information processing facilities should have a secure, physically sound perimeter with suitable controls and restrictions allowing access to authorized staff only. CCTV and audible alarm systems should be active in areas where critical servers are located, such as in the data center.
8. Observance and maintenance of the physical security of rooms and offices where PCs and/or critical information processing equipment is located needs to be a paramount consideration. For example, do not house critical equipment in publicly accessible locations, close to windows, in areas where theft is a high risk. Locate servers and business critical equipment in locations with adequate environmental and fire controls.
9. Access to information processing systems will only be allocated to staff following any required legal/ Pragmatic Solutions checks. If required, usage

policies will also need to be signed by staff.

10. All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.
11. Access to and knowledge of key fobs, door lock codes or access to keys for locks, are restricted to authorized personnel only and must not be shared with any unauthorized person.
12. Access codes used for secure locking mechanisms must be changed every three months as a minimum or more regularly as specified by the location manager in line with professional best practice. Outside of the company, a record should be kept in a secure location of when the dates when the access codes are updated.
13. If electronic door locks/key fobs are in use they must be issued to authorized staff on an individual basis, be fully registered to that individual and only used by that individual. The key fob must be deactivated immediately when no longer required and registration details updated accordingly.
14. Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.
15. All Pragmatic Solutions / Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this procedure.
16. Personal, special access visits from relatives or acquaintances of personnel are not permitted within secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure.
17. Equipment should be sited to minimize unnecessary, unauthorized access into work areas. For example, refreshment units or office machinery designed for visitors should be placed in publicly accessible areas only.

Access to the Pragmatic Solutions application will be from these categories of users:

- Pragmatic Solutions' employees
- Pragmatic Solutions' Support - to manage the system and user accounts
- 3rd Party Support - to manage day-to-day support

It must be possible for each category of users to freeze or restrict account usage. Pragmatic Solutions' / Support must be able to freeze or restrict access to all accounts.

Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Pragmatic Solutions assets, or an event which is in breach of the company's security procedures and policies. All Pragmatic Solutions employees, elected members, partner agencies, Third Parties and vendors have a responsibility to report security incidents and breaches of this

policy as quickly as possible through the company's Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access the Information Systems of the company. Pragmatic Solutions will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the disciplinary procedures.

This document forms part of the company's Information Security Policy and as such, must be fully complied with.

8. Information systems acquisition, development & maintenance

Policy objective

Ensure that security is an integral part of all information systems within Pragmatic Solutions and its clients.

Procedure guidelines

- Business requirements for new information systems or enhancements to existing systems must specify the requirements for security controls.
- Data and databases used in test or staging environments must be sanitized and not contain any sensitive or confidential information.
- An awareness of new security vulnerabilities must be maintained as they are discovered and assess the impact on all environments.
- The environments should be regularly checked for compliance with security policy and initially checked before go-live.
- The environments should be regularly tested, on at least an annual basis and initially before go-live.

Production environment

- All production environments must be designed and operated in a multiply redundant configuration so that there is no single point of failure in the production infrastructure.
- All production systems must be subject to a level of operating system hardening and not run any unnecessary services.
- All production systems must have a patch program in-place to identify any software patches required and install them as required.
- The production environment must not contain components with known vulnerabilities unless a risk assessment has been made and signed-off.

Application design

- Application software must be robust, self-checking, and not vulnerable to invalid user input or the deliberate or accidental corruption of information.
- All applications must protect the confidentiality and integrity of the data that they use or rely on.
- The application must not be vulnerable to a simple Denial of Service attack such as an automated "first page" player registration.
- The application must generate a secure audit trail of all activity which is digitally signed by the application and can be shown to be unmodified in a Court of Law.
- The application software must validate all customer-requested data changes by sending an automated email to the customer. This email must be responded to by the customer before the requested change to customer data can be made.
- The application must be able to reliably determine the country of origin of a player during the sign-up operation.
- The application must take all possible steps to ensure that player sign-up is legal in the country of origin of the player.
- The application web site must comply with common content-rating guidelines so that it can be blocked, if required, by relevant authorities.
- The application must comply with all relevant data protection legislation, particularly about personal data.

Source code

- Access to the application source code must be restricted to authorized individuals only and the source code must be encrypted outside the office environment (Laptops etc.)
- Application source code must not contain embedded authentication credentials.
- Application source code must not be held on any systems in the production environment, and there must not be an application build environment installed on the production systems.
- An independent trusted 3rd party must review the production code to ensure that there is no functionality present which is not documented.
- Production environment or source code changes must be logged using a formal change management system and be subjected to peer review and approval before being released into the staging or test environment.
- Production environment changes must always contain an approved back-out plan in the event of unforeseen consequences of the change.
- Release of code from the staging environment to the live production environment must involve multiple levels of sign-off and agreement.
- A complete and updated backup of the source code is kept locked in a safe by Pragmatic Solutions.

9. Information security incident management

Policy objective

All incident detections and responses must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Incident Manager.

Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

All Pragmatic Solutions' employees, contractors and 3rd parties must be required to note and report any observed or suspected security weaknesses in systems or services.

Procedure guidelines

- Incident Identification: Staff must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures.
- Reporting and Incident Declaration Procedures: Security should be notified immediately of any suspected or real security incidents involving Pragmatic Solutions computing assets, particularly any critical system/application. If it is unclear as to whether a situation should be considered a security incident, the responsible person should be contacted to evaluate the situation.
- Notification obligations: Management with the assistance of the legal counsel, the DPO and an IT specialist will analyse data breach/incident and decide if should be notified, in which way, to whom and when.
- Incident Severity Classification: Defined levels should be used to determine what response the Security will take.
- Incident Response: Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.
- Root Cause Analysis and Lessons Learned: Team should meet to review the results of the investigation conducted, to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan.
- Service Level Agreement: The purpose of the SLA is to set the minimum levels of availability of the Platform to be provided by Pragmatic Solutions to its clients, and the manner by which any downtime or faults in the platform will be reported and processed by PS.

10. Business continuity management

Policy objective

Counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Procedure guidelines

- A managed process must be developed and maintained for business continuity that addresses the business and information security requirements needed for Pragmatic Solutions' business continuity.
- Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences.
- Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
- A single framework of business continuity plans must be maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance.
- Business continuity plans must be tested (if possible) and updated regularly to ensure that they are up to date and effective.
- Business Continuity Plan is currently in place for Pragmatic Solutions' operations however outsourced partners have separate disaster recovery measures and procedures in addition.

11. Compliance

Policy objective

Avoid breaches of any law, statutory, regulatory or contractual obligations.

Procedure guidelines

- Statutory, regulatory and contractual requirements must be explicitly defined, documented and kept up to date.
- All intellectual property rights and licensing terms for the use of proprietary software products must be respected and enforced within Pragmatic Solutions and by all contractors and 3rd parties.
- Critical data must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.
- Data protection and privacy must be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses.

- Managers must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

12. Virtual Private Network (VPN) Policy

Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the corporate network.

Scope

This policy applies to all Pragmatic Solutions employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Pragmatic Solutions network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Policy

Approved Pragmatic Solutions employees and authorized third parties (clients, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Pragmatic Solutions internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by network operational groups.
6. All computers connected to Pragmatic Solutions internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

7. VPN users will be automatically disconnected from Pragmatic Solutions network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Pragmatic Solutions-owned equipment must configure the equipment to comply with Pragmatic Solutions VPN and Network policies.
10. Only approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Pragmatic Solutions network, and as such are subject to the same rules and regulations that apply to Pragmatic Solutions-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

Policy Compliance

Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic demonstrations, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner

Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

13. Desktop and Laptop Computer Security

Overview

Most of Pragmatic Solutions business is conducted with the use of desktop or laptop computers dedicated to a single user's activity. It is essential to protect Pragmatic Solutions information assets created, gathered, shared or stored with desktop and laptop computers, related computer media (e.g. diskettes, CDRoms, Personal Digital Assistants (PDAs), flash drives, etc.) and peripheral equipment such as fax machines, printers and copiers.

Purpose/Rationale

The purpose of this policy is to set security provisions for securing desktop and laptop computers, related computer media and peripheral equipment.

Applicability

All individuals granted access to the Pragmatic Solutions network and information systems including but not limited to full and part-time employees, temporary workers, volunteers, contractors, and those employed by others to perform Pragmatic Solutions work, are covered by this policy and shall comply with this and associated policies, procedures and guidelines.

This policy includes all computers (e.g., desktops and laptops), stand alone as well as those connected to the Pragmatic Solutions Network.

The same physical and technical security measures shall be implemented for mobile and remote computers.

Failure to Comply

Failure to comply with information security policies or other associated policies, standards, guidelines, and procedures may result in disciplinary actions up to and including termination of employment for employees or termination of contracts for volunteers, contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Policy

Pragmatic Solutions will ensure reasonable physical safeguards to maintain desktop and laptop computers and peripheral equipment in such a way to avoid inadvertent disclosure of Pragmatic Solutions information.

Pragmatic Solutions shall be responsible for secure installations, configurations, distribution, management and removal from service, of Pragmatic Solutions desktop and laptop computers. Pragmatic Solutions must document if these responsibilities are assigned to another program area or office.

Pragmatic Solutions may withdraw permission for any or all business or personal uses of its network or information systems at any time.

Securing Desktop and Laptop Computers

Individuals granted access to the Pragmatic Solutions Network or information systems shall secure desktop and laptop computers from inadvertent or unauthorized access.

- When leaving a desktop or laptop computer unattended, users shall apply the "Lock

- Workstation" feature (ctrl/alt/delete, enter) where systems allow.
- Unattended desktop and laptop computers shall be secured from viewing by password protected screen savers.
- Desktop and laptop computers shall be set to activate the automatic screensaver feature after a period of non-use. The period of non-use shall be for no more than five (5) minutes.
- Desktop computer users shall store confidential and sensitive information on a networked drive (shared directory on the Pragmatic Solutions Network) and not the user's hard drive.
- Laptop computers that store confidential or sensitive information must have encryption technology. Users should contact Pragmatic Solutions to request or confirm that their standard encryption technology is installed on their assigned laptop computer.
- Desktop and laptop computers and monitors shall be turned off at the end of each workday.
- Desktop and laptop computer users shall not disable or alter security safeguards, such as virus detection software, installed on Pragmatic Solutions desktop or laptop computers.

Physical Security Measures

Physical security measures shall be used to secure laptops, computer media, and other forms of information storage media containing confidential or sensitive information.

- Mobile laptop computers actively connected to the network or information systems must not be left unattended.
- Laptop computers left in a vehicle shall not be visible. If possible, the laptop should be stored in a locked trunk. (Weather conditions should be considered when leaving electronic equipment in a vehicle for long periods of time.) Unattended vehicles shall be locked always.
- Mobile laptop computers, computer media and any other forms of removable storage (e.g. diskettes, CD ROMs, zip disks, PDAs, flash drives) shall be stored in a secure location or locked cabinet when not in use.
- Other information storage media containing confidential data such as paper, files, tapes, etc. shall be stored in a secure location or locked cabinet when not in use.

Peripheral Equipment

Peripheral equipment (e.g. printers, faxes, copiers) that store, produce and/or transfer confidential or sensitive information shall be protected from inadvertent or unauthorized access.

- Fax and telex machines that store or transmit confidential or sensitive information shall be placed in secure locations and monitored.
- All documents containing confidential or sensitive information shall be cleared from printers and copiers immediately.

Unauthorized Software

- Individual users shall not install or download software applications and/or executable files to any Pragmatic Solutions desktop or laptop computer without prior authorization from Pragmatic Solutions.
- Pragmatic Solutions shall make available to users, a list of authorized and accepted software and applications approved by them.

Viruses

- Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).
- Suspected viruses should be reported immediately.
- Viruses shall not be deleted without expert assistance unless instructed by Pragmatic Solutions.
- The Company shall inform the relevant authorities as soon as malicious code is discovered in the system and take any and all necessary steps to ensure that the malicious code does not affect the application.

Monitoring of desktop and laptop computers.

- Pragmatic Solutions reserves the right to monitor individual user desktop and laptop computers at random or for cause.

Technical Security

Desktop and laptop computers shall be configured to reduce the risk of inadvertent or unauthorized access to Pragmatic Solutions information and systems.

- All Pragmatic Solutions desktop and laptop computers shall be configured according to the Pragmatic Solutions desktop and laptop configuration standards.
- User identification (name) and authentication (password) shall be required to access the operating system of all desktop and laptop computers whenever turned on or booted.
- Terminal sessions shall be configured to log a user off the system during extended periods of non-use. The period of non-use shall be for no more than 60 minutes.

- Local hard drives shall not be accessible when a desktop or laptop computer is booted from mobile media, e.g., a diskette or compact disk.
- All information stored in a shared directory on the Pragmatic Solutions Network shall be backed up daily by Pragmatic Solutions.
- Pragmatic Solutions standard virus detection software shall be installed on all desktop and laptop computers, mobile, and remote devices and shall be configured to check files when read and routinely scan the system for viruses.
- Desktop and laptop computers shall be configured to log all significant computer security relevant events. (e.g., password guessing, unauthorized access attempts or modifications to applications or systems software.)

Policy exceptions

Pragmatic Solutions shall be authorized to approve or deny policy exceptions regarding elements of any Information Security Policy. Policy exception requests shall be submitted electronically or in hard copy form to Pragmatic Solutions.

14. Media and Equipment Disposal

Purpose

The disposal of media, computer equipment, and computer software can create information security risks. These risks are related to the potential unauthorized disclosure of electronics, protected information or other sensitive data, violations of software license agreements, and unauthorized disclosure of intellectual property that could be stored in hard disks and other storage media.

This policy will govern the requirements of secure disposal of media containing sensitive data or protected information, by establishing a process through which the secure removal of sensitive data or protected information is achieved on all media used within Pragmatic Solutions prior to disposal.

This Equipment and Media Disposal Policy is designed to protect organizational data, equipment or media being removed from service. This policy is intended to protect the employee and the company by protecting data to meet confidentiality and privacy requirements.

Scope

This policy applies to all Pragmatic Solutions employees who authorize the disposal, handle the media or devices intended for disposal, or who are directly responsible

for the disposal of media and devices containing sensitive data or protected information. This policy covers all fixed and removable storage devices owned by Pragmatic Solutions. This includes but is not limited to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), and PDAs. Any storage devices currently available, or that become available in the future due to new technology, are also covered by this policy.

Responsibility and requirements

Disposal and sanitation methods

- All electronic devices and media equipment, including storage media in personal computers and other hardware containing sensitive data or protected information, will be sanitized prior to disposal.
- The proper sanitation method depends on the type of media and the intended disposition of the media.
- Media containing sensitive data or protected information must be degaussed or destroyed prior to disposal so that data will not be retrieved and reused.
- Non-functioning and/or non-writable media containing sensitive data or protected information must be physically destroyed if degaussing or another sanitization is determined to be inadequate.
- Media not containing sensitive data or protected information can either be sanitized or destroyed to an appropriate condition.
- Disposal of media requires authorization and tracking by the data owner of record.
- All methods of media disposal will be in agreement with information security best practices, while also considering cost-effectiveness and the safety of employees.

Office Responsibilities

- Each office will designate an individual(s) to be responsible for assuring that protected information, as well as the hardware or electronic media on which it is stored, is properly destroyed and cannot be re-created.
- Each office will designate an individual(s) to oversee the monitoring process.
- Each office will designate an individual(s) to document disposal information beginning with the point of designation for destruction to final disposal.

- The chain of custody of the data will be established and maintained in the disposal documentation and will clearly identify the asset or media to be disposed, as well as the individual(s) responsible for its disposal.
- Disposal information will be kept for a period to be specified by Pragmatic Solutions.

Policy and Operating Procedure (OP) Updates

- Updates to Information Technology (IT) policies and OPs concerning Media Controls will be made on a periodic basis.
- All employees responsible for disposal activities will receive periodic training on IT policies and procedures on the use of software and tools utilized to prepare and audit media and devices for disposal.
- Disposal activities will be audited on a regular basis by a designated individual(s) to verify compliance with IT policies.

Enforcement Authority

The Information Security Team (IST) is designated to monitor and provide initial enforcement of Pragmatic Solutions information security program and IT policies.

Violations and Disciplinary Action(s)

- All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.
- The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to the responsible Director for appropriate action.
- As determined by the responsible Director, instances of abuse or misconduct, depending on the circumstances, will be referred for further investigation.
- Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions to this policy may be subject to: (1) disciplinary action as outlined by Pragmatic Solutions; or (2) criminal prosecution.

Definitions

- Degauss – To demagnetize data from storage devices to destroy the media so it is no longer usable.
- Device – Including but not limited to personal computers, laptops, handheld units (PDA's).

- Disposal - The final disposition of electronic data, and/or the hardware on which electronic data is stored.
- Employee - Individuals employed on a temporary or permanent basis by Pragmatic Solutions; as well as contractors, contractor's employees, volunteers, and individuals who are determined by Pragmatic Solutions to be subject to this policy. For this policy, this also refers to anyone using a computer connected to the Pragmatic Solutions network.
- Media Controls - Formal, documented, policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.
- Sanitization - The process of rendering data harmless

15. Removable Media Policy

Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Pragmatic Solutions and to reduce the risk of acquiring malware infections on computers operated by Pragmatic Solutions.

Scope

This policy covers all computers and servers operating in Pragmatic Solutions.

Policy

Pragmatic Solutions staff may only use Pragmatic Solutions removable media in their work computers. Pragmatic Solutions removable media may not be connected to or used in computers that are not owned or leased by the Pragmatic Solutions without explicit permission of the Pragmatic Solutions InfoSec staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Pragmatic Solutions Acceptable Encryption Policy. Exceptions to this policy may be requested on a case-by-case basis by Pragmatic Solutions exception procedures.

Policy Compliance

Compliance Measurement: Pragmatic Solutions will verify compliance to this policy through various methods, including but not limited to, periodic demonstrations, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions: Any exception to the policy must be approved in advance.

Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

16. Encryption Key Protection Policy

Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys use to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

Decentralize encryption and decryption

One critical issue in designing a data protection plan is whether encryption and decryption will take place locally and be distributed throughout the enterprise, or will be performed at a central location on a single-purpose encryption server. If encryption and decryption are distributed, the key manager must provide for the secure distribution and management of keys.

Solutions that provide encryption at the file, database field, and application level provide the highest level of security while allowing authorized individuals ready access to the information. Decentralized encryption and decryption provide higher performance and require less network bandwidth, increase availability by eliminating points of failure, and ensure superior protection by moving data around more frequently but securely.

Centralize key management with distributed execution

A solution that employs a hub-and-spoke architecture for distributed key management allows encryption and decryption nodes to exist at any point within the enterprise network. Spoke key-management components are easily deployed to these nodes and integrated with the local encryption applications. Once the spoke components are active, all encryption and decryption of the formerly clear text data is performed locally to minimize the risk of a network or single component failure having a large impact on overall data security. The key manager should manage the generation, secure storage, rotation, export, and retirement of the keys used for encryption at the spokes.

Support multiple encryption standards

Even if you choose specific encryption standards for your organization, you may find that mergers and acquisitions or the need to work with business partners in your ecosystem will require support of other standards. Choosing a security solution that supports all industry-standard encryption algorithms ensures your organization will conform to government and regulatory requirements now and in the future.

Centralize user profiles for authentication and access to keys

A “user” is any application or person requiring access to sensitive data. Access to these resources should be based on user profiles in the key manager. Users can be assigned and issued credentials (for example, RSA certificates) to provide access to encryption resources associated with their user profile. User profiles are managed through an administrative role in the key manager. In compliance with the PCI DSS mandate and as a best practice, no single administrator or user has access to the actual keys themselves.

Do not require decryption/re-encryption for key rotation or expiration

A key profile should be associated with every encrypted data field or file. This key profile allows the application to identify the encryption resources that must be used to decrypt the data field or file, making it unnecessary to decrypt and then re-encrypt data when keys change or expire. The current key will be used to encrypt freshly created data. For existing data, the key profile will be looked up to identify and load the key that was originally used for the encryption.

Keep comprehensive logs and audit trails

Extensive audit logging that occurs in every component of the distributed architecture is an important component of key management. Every access to sensitive data must be logged with details about the function, the user (individual or application), the encryption resources utilized, the data accessed, and when the access took place.

Use one solution to support fields, files, and databases

One benefit of the distributed execution model is that the security software doesn't know or care what kind of data it is encrypting. To get started, define which fields need to be protected and specify how they are to be protected. Once activated, information is available based on user rights, allowing access (to the full value or a predefined masked value) or denying access. Look for a security solution that operates without requiring any alternation of any field sizes.

Support third-party integration

Enterprises often have a large number of external devices (i.e., POS terminals) dispersed throughout their network. These devices do not typically have standard database-oriented applications and are dedicated to a single function using proprietary software. Using a security solution that integrates with third-party applications will protect confidential information as it moves throughout your organization's extended network.

17. Password Management

The password management deals with allocation, regulation and change of password rules of the organization. Organizations face significant security exposure during routine IT operations. For example, dozens of system administrators may share passwords for privileged accounts on thousands of devices. When system administrators move on, the passwords they used during their work often remain unchanged, leaving organizations vulnerable to attack by former employees and contractors.

Weak password management means that the most sensitive passwords are often the least well defended. The need to coordinate password updates among multiple people and programs makes changing the most sensitive passwords technically difficult. Inability to secure sensitive passwords exposes organizations to a variety of security exploits. Strong, manual controls over access to privileged accounts may sometimes create unanticipated risks, such as impaired service in IT operations and escalation of physical disasters from one site to an entire organization. Inability to associate administrative actions with the people who initiated them may violate internal control requirements.

18. Data Classification

Data Classification

The security requirements set forth in this document are high level requirements that establish the minimum standards necessary for each DCL (DLC means Data Classification Level). To be effective, these requirements must be used in conjunction with other industry standards and best practices.

Systems

All server-based systems, including personal computers when configured as a server, must be administered by a qualified information technology professional and meet the security guidelines established for each data classification level. Each system must be classified at the highest data classification level of the information residing on a given system. For servers utilizing a database, the data residing in the database must be considered as part of the overall system for classification purposes.

Applications

For this document, an application is a browser-based or proprietary application typically used to allow multiple users to read, access, share, modify, input or retrieve data, from a server-based system. Applications, whether provided by a vendor or developed internally, must meet the application security requirements established for each DCL.

The standards in this document do not cover office productivity software, such as Microsoft Office, or other software packages installed for use only on individual workstations.

Exceptions

Due to budget, functional and technology limitations, exceptions to the standards in this document may be required. Exceptions must be approved and documented by the CTO and its team. Exceptions must also be eliminated as soon as is reasonably possible.

DCL Definitions

DCL1--Public

Public data has been explicitly approved for distribution to the public by the data owner or through some other valid authority. Disclosure of public data requires no authorization and may be freely disseminated without potential harm to the company or its affiliates.

Examples: Advertising, product and service information, published research, presentations or papers, job postings, press releases, instructions, training manuals, the terms and conditions of the gaming platform, odds, news, banner.

DCL2--Sensitive

While some forms of sensitive data are available to the public, the distinction between public and sensitive data for this DCS is in how the information is made available. Therefore, sensitive data must be protected by authentication or identity verification and includes information that would not be openly shared with the

public. Sensitive data is intended for use within the company or within a specific workgroup, by the owner (for example the user itself), department or group of individuals with a legitimate need-to-know. Unauthorized disclosure of this information could adversely impact the company, individuals or affiliates.

19. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Pragmatic Solutions or our clients' information, or an event which is in breach of Pragmatic Solutions' security procedures and policies.

All employees and third-party suppliers have a responsibility to adhere to this policy and report security incidents and breaches of this policy as quickly as possible through Pragmatic Solutions' Incident Reporting Procedure.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Companies contracted to Pragmatic Solutions found to be violating this policy will be deemed to be in breach of contract.

20. Revision and update of present policy

Pragmatic Solutions understands the importance of this policy and the manner it affects its business and employees. For the information of this policy to remain up to date, the policy will be revised and updated yearly or whenever required during the year.

Employees will be informed about possible new information that revised policy might bring.

VERSION HISTORY

Summary	Version	Date	Author
Initial draft – creation of the document	1.0	9 January 2018	Compliance department
Policy review and update	1.1	14 Mar 2019	Flavia Dumitru
Policy review	2.0	17 Oct 2019	Flavia Dumitru

Updates to Incident Response procedure	2.1	12 Nov 2020	Flavia Georgescu
Policy review and template update	2.2	12 Nov 2021	Flavia Georgescu
Annual review	2.3	Nov 2022	FG
Annual review	2.4	Nov 2023	FG
Annual review and policy refresh	2.5	Nov 2024	FG
Annual policy review	2.6	Oct 2025	FG