Information Security Policy

Preface

Applicability

Objective: To establish security implementation practices for the protection of Parenta information assets on network environments within the Parenta Group and all associated subsidiaries.

Scope: This standard defines the requirements for network infrastructures and system services, where Parenta's internal business processing is performed and where availability of the infrastructure and system service is required by and committed to multiple users. This scope also extends to any Parenta Systems that are hosted and managed by 3rd Party companies under an agreed and Documented Service Level Agreements.

Compliance: Compliance with this Standard is mandatory and subject to audit inspections. Any non-compliance must be documented in a risk acceptance.

Exceptions: Systems that are used to provide demonstration, education, or test services for those individuals authorised to use Parenta internal Information Technology services are not required to implement the rules and processes described in this standard. However, these systems must prevent unauthorised access to and from Parenta networks and must limit physical and logical access to only members of the work group.

Document Control

0.1 Change History

ISSUE	DATE OF ISSUE	COMMENT
1.0	17 March 2009	First Draft Allan Presland
	18 March 2009	Initial Review
1.1 23	17th March 2011	Updated By Richard China
1.2 2	4th April 2011	Reviewed By Allan Presland

0.2 Change Forecast

17th March 2011

0.3 References

- Discussion with Parenta
- RFC 2504
- The Data Protection Act 1998
- DTI – Protecting Business Information
  http://www.dti.gov.uk/PROTECT/confidential/intro.htm
- British Standard – BS7799 & ISO27001

0.4 Document Owner

This document is owned by: Allan Presland

Accountability for Updates is by: Davinder Mann

0.5 Definition

For the purposes of this document, the term Parenta is used generically to cover Parenta Group Ltd, and all Parenta Group subsidiary companies.

0.6 Data Classification

Data	Classification
Client Confidential	Any and all data belonging to clients to include all of their private data.
Parenta Confidential	Any and all data relating to Parenta's clients to include their name and addresses, access codes and account history.
Parenta Internal	Any and all data required by staff to undertake their roles & responsibilities
Parenta management	Any and all data which is restricted to specific Parenta personnel, such as payroll data, accounts data or information for the Directors
3rd Party Copyrighted and Protected	Any and all data that is provided by Parenta 3rd Parties suppliers or is procured by Parenta as part of its service and product offerings
Public Domain Data	Any Data that is obtained freely and is in the Public Domain

Table of Contents

Introduction

This document details Parenta's Information Security Policy that all staff employed by the company must adhere to when dealing with Customers and Learners

Good security policy is a business enabler. It allows managers and departments to assess and monitor not only the security of their systems but also assists in maintaining the integrity and availability of network as a whole

Each employee has an individual responsibility to keep information about the company's customers and learners confidential. This means passwords are kept secure, and documents printed which are labelled as confidential are treated as such.

This document comprises different sections, each covering a specific aspect of Security. The sections are as follows,

- Physical Access Controls
- Logical Access Controls
- Security Status Checking
- Security Incident Reporting
- Legal requirements
- Data Protection Act
- The Internet
- Back-up procedure

Parenta and the Law

All employees of Parenta are responsible for respecting and adhering to local and international law(s). Any attempt to break those laws through the use of the system may result in litigation against the offender by the proper authorities. If such an event should occur, Parenta will comply fully with the authorities to provide any information necessary for the litigation process.

1 Physical Access Controls

Theft or damage to information processing resources, unauthorized disclosure or erasure of Parenta information, and interruption of support for Parenta business processes are all risks that managers who own or are responsible for information processing must evaluate. Because physical access to information processing resources exposes us all of these risks, we must instigate controls to interdict physical access controls that are commensurate with the risk and potential loss to the company.

1.1 Controlled Access Areas

This standard establishes definitions and requirements for Controlled Access Areas within Parenta's Internal space. These areas are used to house computing facilities, portable storage media, and remote printers.

Controlled Access (1) Areas - These areas must be located within Parenta's Internal Space. In this document, these areas are referred to as CA(1) areas and must include the following additional controls:

- The area owner must be clearly identified
- The area must be locked at all times
- Access to the area must be restricted to only those individuals authorized by the area owner

Controlled Access (2) Area - These areas must be located within Parenta Internal space. In this document, these areas are referred to as CA(2) areas and must include the following additional controls:

- The area owner must be clearly identified
- The area must be locked,
- Access to the area must be restricted to only those individuals authorized by the area owner
- Access to the area must only be allowed from Parenta Internal space, and emergency exit doors must be alarmed
- Exterior windows are not permitted in ground floor unless polycarbonate glazing or other shatter resistant glass is used.
- Access to the area must be controlled by electronically controlled access (CAS) unless specifically exempted by the area owner's Director or equivalent level executive.

1.2 Local Area Networks

LANs should be designed to limit the aggregation of data that is subject to unauthorised interception (e.g., packet sniffer attacks). A switched network utilising a hierarchical design is one example of how this could be achieved.

Note: The use of sniffer-like devices on Parenta premises is prohibited except for authorized individuals with valid business reasons.

1.3 LAN Infrastructure Components

Table 1. Physical access requirements for network infrastructure components

Component	Minimum security requirements
LAN management systems	CA(1) area or in an office room that is locked when unattended
Bridges, Gateways, Repeaters, Routers, Wiring hubs, Wiring closets, Physical Firewall	CA(1) area
Ports	No active ports are allowed in Parenta Public Space when not under Parenta supervision. Active ports, whether or not a system or device is connected, are allowed on user LAN segments within Parenta Internal Space. If a hierarchical LAN design is used, active ports are not allowed on non-user LAN segments (e.g., backbones), unless the parts are in a CA(1) area.
Modems	The same physical access protection requirement as the system or infrastructure components to which they are connected. Note: Modems are generally used as part of authorised 3rd Party support

1.4 LAN Connected Systems

Table 2. Physical access requirements for network connected systems

System	Minimum security requirements
Systems that are essential to Parenta	CA(2) area
All other systems covered by this Standard	CA(1) area or in an office room that is locked when unattended

Note: System and case keys need not be removed.

1.5 Storage Media

Storage media includes magnetic tape and removable and non-removable optical or magnetic disks and cartridges. A storage media custodian is an individual who has accepted the responsibility for storage of removable media on behalf of other people. Unlike media used for normal system and data backup purposes, media placed in custodial care:

- Is routinely mounted and dismounted for business processing, or
- Contains information identified as essential for records retention, or
- Contains information identified as essential for disaster recovery.

Therefore, it must be possible to account for the movement and control of media in a custodian's storage media library.

Note: In LAN environments, data is typically created, accessed, and stored on magnetic disks on LAN workstations and servers. This data generally remains online and is not placed on removable media (other than for backup purposes) or routinely mounted and dismounted for business processing. (Hot swappable storage media is not considered removable.)

1.5.1. Classification of Storage Media

Classification of information is the data owner's responsibility. Media containing Confidential information should be marked accordingly wherever possible. Non-removable media need not have a classification label on the actual device.

Media used for backups, records retention, or disaster recovery may be marked or labelled with a general statement:

"Property of Parenta - may contain Parenta Confidential information and must be protected from unauthorized use or access. Must not be removed from Parenta control without proper authorization and without marking with the Parenta Confidential information label."

This label may also be used on media transported to and from or stored in an authorized retention facility and on locked containers used to transport such media.

1.5.2. Physical Protection of Storage Media

Media under custodial control and media used for backup, records retention, or disaster recovery must be stored in CA(1) or CA(2) areas, or in an office room that is locked when unattended, or in a locked cabinet in Parenta Internal Space when unattended.

Tape drives and media handling devices (e.g., "tape robots", direct access storage, and "juke boxes") need not be locked when located in a CA(1) or CA(2) area or an office room that is locked when unattended.

Media used for normal system and data backup purposes must be kept separate from media placed under custodial control and must be managed with prudent business controls to ensure media availability in case recovery is required, but need not be included in the inventory control process that is applied to media placed under custodial care.

Note: If media separation is not possible, all media must be included in the custodial media inventory control process described below.

The movement of media to and from an authorized media retention facility must be accounted for using transmittal records or an equivalent process.

1.5.3. Custodial Media Inventory Control

Custodians of storage media are responsible for implementing inventory control procedures and for performing an accurate inventory reconciliation of the media in the custodial media library at least annually. A media inventory must also be conducted when there is a change in tape library ownership or outsourcing of the tape library.

Note: At least one person not directly involved in the media operation must conduct the inventory process; however, the custodial media librarian may participate.

The inventory reconciliation must be able to demonstrate the following:

- Beginning inventory (prior ending inventory)
- Plus media in (received from other locations)
- Minus media out (sent to other locations)
- Plus new media added to library
- Minus scrapped media
- Equals current ending inventory (total number of tapes managed by the library)

All discrepancies must be reported to management and accounted for.

All media used to support the custodial media library, including opened blank or scratch media in media handling devices and robot controlled storage libraries, must be included in the inventory reconciliation.

The manager responsible for the custodial media library must sign the completed inventory documentation.

The last inventory reconciliation and supporting documentation (including the previous signed total inventory reconciliation page), must be retained.

1.5.4. Residual Information

Residual Parenta Confidential data must be made unreadable prior to disposal or non-Parenta use.

1.6 Printers

Control of print output is the responsibility of the end user. The end user must comply with the print requirements specified in the "Computer Security Guidelines for Parenta Employees".

2 Logical Access Controls

Logical access controls include the following primary topics. The requirements for each are identified in this section.

- Identify and Authenticate Users: Ensure that a unique identifier (e.g., user id) can be associated with each potential user of Parenta systems. When the user enters the system, ensure that a further level of identification (e.g., a password) verifies that the user is who he or she claims to be.
- Define and Protect Resources: Ensure that each resource on the system can be identified, that access to the resource can be allowed at the appropriate levels for authorized users, and that access is denied for unauthorized users.
- System and Security Administration: Ensure that only authorized users can set, modify, or disable system security functions.
- Log Access Attempts: Ensure that an audit record can be created for each successful or unsuccessful access attempt to the system or to protected resources on the system.
- Report Access Violations: Ensure that unauthorized access attempts to systems or information can be recognized as violations, either immediately or on subsequent analysis.

2.1 Identify and Authenticate Users

2.1.1. User Ids

Access authority to internal systems must be based on current need and controlled by verifying the identity of the user or application. User ids must be identifiable to an individual.

Notes: Administrator user ids or passwords give access to functions that need to be used potentially by a group of people. In such cases, those user ids or passwords may be shared by the group under the following conditions:

- Wherever possible, passwords should not be shared, so individual accountability for the initial user id logon is maintained.
- Unauthorised use of the user id or password is prevented.
- The user id must not be an individual's user id that could contain information the group has no need to know.

In these specific cases and under these conditions, there is no requirement to document a formal risk acceptance for shared user ids or passwords.

2.1.1.1. User ID Authorization

A process must be in place for authorizing users to computer systems. This process must include notifying the manager associated with the user.

2.1.1.2. Management Notification to Revoke

When a user leaves the company, goes on leave of absence and is not expected to return to regular employment, or no longer has a valid business need, the user's manager must notify the system owner. The system owner must have a process or technical controls in place to prevent the user's access to the system(s) immediately following the manager's notification.

2.1.1.3. Quarterly Review

A quarterly process must be in place to ensure the removal from Parenta's user ids and access capabilities of individuals no longer in the employ of Parenta. This process serves as a safeguard in the event that management failed to notify system owners when an individual's employment ended.

2.1.1.4. Annual Revalidation

An annual process must be in place for revalidation of user ids. Revalidation can be accomplished using a report sent to management that lists employees on the system. Management must follow-up on discrepancies with the system owner.

2.1.2. Passwords

The robustness of the password is the most important mechanism available to protect systems. The password rules identified in this section are applicable to all system and subsystem logon/login passwords.

Note: In many cases, default passwords are shipped with operating systems and program products for use during system and product installation and setup. Without exception, default passwords must be changed as soon as possible during or following their initial use.

Passwords must:

- Be at least six positions in length, when supported by the technology
- Contain at least one alphabetic and one non-alphabetic character
- Contain a non-numeric character in the first and last position
- Contain no more than three identical consecutive characters in any position from the previous password
- Contain no more than two identical consecutive characters
- Not contain the user id as part of the password
- Be changed at least once every 90 days.
- Not be reused until after at least four iterations.
- Not be shared unless individual accountability is maintained.

Notes:

"Pass phrases" or "smart cards" are acceptable alternatives to passwords.

Passwords that have not been changed in 90 days but which are in an expired state are not in violation of the password change interval requirement.

2.1.2.1. Invalid Password Attempts

Controls must be in place to prevent an unlimited number of invalid logon password attempts (i.e., password hacking).This must be accomplished by either revoking or locking the user id upon the fifth consecutive invalid attempt or by using a logon inductor to exponentially increase the amount of time between sign on screens.

2.1.2.2. Resetting Passwords

A process must be in place to reset passwords. The process must either include provisions for positive identification of the requester, or the new password must be sent to a manager.

2.1.3. Business Use Notice

Parenta wishes to notify individuals that unauthorized use of Parenta systems is a violation of Parenta's rights and to remind Parenta employees that Parenta's internal systems must only be used for conducting Parenta's business or for purposes authorized by Parenta management. Therefore, the notification that

"Parenta's internal systems must only be used for conducting Parenta's business or for purposes authorized by Parenta management"

must be presented to people logging onto Parenta processors during the identification and authentication process if the Parenta processor is running an operating system can provide such a notification.

Note: Displaying the business use notice at any point from the initial system logo presentation until the user completes the sign on process meets the "during the identification and authentication process" criteria.

It is also advisable that the following sentence be added to the business use notice when it is displayed:

"Use is subject to audit at any time by Parenta management."

2.2 Define and Protect Resources

Data objects (or assets) can take the form of text, programs, or data. Objects belonging to individuals or groups are user resources. Objects that are related to system services or functions are operating system resources.

2.2.1. Classification of Data Objects

Data classification provides Parenta with the legal and physical basis for protecting against loss, misuse, unauthorized disclosure, etc.

When data objects are created by the owner, they must be evaluated to determine which classification is required for the object, and thus which level of protection is necessary.

The owner of a data object is responsible for its classification.

2.2.2. Protecting Parenta Confidential Information

Confidential information is classified as information which, if disclosed to an unauthorized people or third parties, would,

- Breach the law
- Breach the confidentiality of the client relationship
- Damage Parenta's bushiness or competitiveness

All information relating to both Parenta’s customers and staff must be treated as confidential, this includes account passwords, access details (for Dial-up accounts or VPNs), addresses, employment records, quotes, tenders and network diagrams, and access codes, etc.

Parenta Confidential information stored on computer diskettes, CD/DVD and tapes must be protected against theft and unauthorized access. Diskettes, CD/DVD and tapes should be stored in a locked area or storage device when they are not in use.

Parenta Confidential printed information must be protected against theft and unauthorized access. (The term printer includes printers and any other device used to create hardcopy output.) Parenta Confidential information may only be printed:

- In a controlled access area, with access based on "need to know”
- In an attended printer facility, where the output is given only to its owner,
- On a printer that is being personally attended.

Data objects that are classified Parenta Confidential must only be made available to individuals with a need to know, and access to the Parenta Confidential objects must be explicitly permitted. If all members of a group have a need to know about a Parenta Confidential object, that group may be granted access to the object.

Note: Access by system support personnel in the course of an activity such as system backups does not require explicit access permission from the user resource owner.

2.2.3. User Resources

The resource owner is responsible for the classification and subsequent protection of resource and for any consequences if the resources are exposed due to insufficient protection.

2.2.4. Operating System Resources

The integrity of operating system resources must be ensured. Operating system resources are those data objects which are part of:

- The system control program and its access control mechanism
- Subsystems and programs

The following default levels of protection must be applied:

- No operating system resources may be updated by a general user, except as required for normal system operations.
- All operating system resources may be read or executed by general users, except when this would assist the user to bypass security controls.

2.2.5. Encryption

When the physical access to data cannot be controlled or the data is of such sensitivity that additional security is required, data can be encrypted to render it unusable for either processing or viewing by unauthorized persons. Encryption Keys are alphanumeric strings that are used as input to a data encryption program. Their use is on a "need-to-know" basis and they are therefore classified Parenta Confidential.

Notes:

Encrypted information retains its original classification and must be protected accordingly.

Miscellaneous use of encryption such as the use of a user id-password string to encrypt logon passwords does not automatically confer the status of "encryption key" to this string.

Most processing environments provide file-level encryption functions that can be invoked by a data owner to secure a file before storage or transmission.

Protection of Encryption Keys

- Access to or distribution of encryption keys must be restricted to people and processes that are authorized and are required to perform the encryption or decryption functions.
- Authorization must be by the owner of the data to be encrypted or decrypted.
- The distribution method must ensure that only authorized persons are provided with the key.
- If the key is unencrypted, it must be transmitted through a separate route from the encrypted data.

- The key must be protected from unauthorized use.
- Use of public key encryption is recommended

2.2.6. Harmful Code

Anti-virus programs must be configured to scan for viral signatures at least once a day and if the software permits it twice daily.

Anti-virus program signature updates must be installed within one week of availability. Checks for new anti-virus updates should be performed daily.

If a system or server becomes infected by a computer virus, the system or server should be isolated from the network until such time as the virus has been eradicated.

Knowingly propagating virus-infected programs within Parenta should lead to disciplinary action.

2.3 System and Security Administrative Authority

System authority is given to an individual by the assignment of attributes, privileges, or access rights that are associated with operating systems and that are required for performing system support and maintenance activities.

Security administrative authority is given to an individual by the assignment of attributes or privileges that are associated with access control systems and that are required for setting and administering system-wide security controls.

The requirements for managing system and security administrative authorities follow:

- Authority beyond that which is available to a general user must be based on a valid business need. Business need is determined by the system. Written justification of business need is not required. These authorities can be implemented by giving access to a group, then ensuring that the members of that group can be individually identified and managed.
- Activity performed using these authorities must be specifically authorized: by management, by a change control process, or must be consistent with the individual's job description. Management must ensure that individuals having these authorities are made aware of this requirement.
- A demonstrable process must be in place to ensure that authority is removed on a timely basis if the user's business need ends.

2.4 Log Access Attempts

The log records specified in this section must be retained for at least 90 days or indefinitely if disk space permits it.

2.4.1. System Access Logs

All successful and unsuccessful logon attempts must be logged if logging is supported by the access control system.

2.4.2. Resource Access Logs

When resource access logging is supported by the platform, the resource owner is responsible for specifying desired logging options.

2.4.3. Activity Logs

Security administrative authority or system authority (i.e., commands used to change operating system resources and commands used to change the security state) must be logged if logging is supported by the access control system. Logging of these activities must never be turned off.

2.5 Report Access Violations

2.5.1. Invalid Logons

A process must be in place for providing reports of invalid logon attempts on request.

2.5.2. Systematic Attacks

A process or controls must be in place for detecting and handling systematic attacks (attempts to logon). A manager or a person designated by management should be notified whenever the number of revokes and invalid logon attempts exceed an installation defined limit.

3 Security Status Checking

All systems must undergo periodic security health checking and penetration testing.

3.1 Security Health Checking

The health checking process must be conducted at least quarterly on systems that are essential to Parenta.

The process must include the verification of:

- Access control system security settings
- The list of users having security administrative authority or system authority
- Operating system resource security settings and status
- Installation and operation of required anti-virus programs.

3.2 Security Penetration Testing

Penetration testing must be conducted annually on systems that are essential to Parenta, as a minimum.

Note: The use of penetration test tools by individuals who are not part of the formal test process is prohibited.

3.3 Security Assurance Reviews

All systems and services that are addressed by this standard must undergo technical security reviews. Reviews of systems and services that are essential to Parenta must be conducted at least once a year. Reviews of a representative sample of all other systems and services must be conducted at least once every 18 months.

The objective of the assurance review is to verify that systems and services are operated in compliance with the security standards that are described in this Standard.

3.4 Misuse of Authority

Individuals who have been granted security administrative authority or system authority are put in a position of trust by Parenta management. It must be recognized that this level of trust does not constitute management approval to operate outside established business controls. Misuse of authority is a violation of trust that cannot be tolerated.

Any deviations from expected and required results that are detected by the security status check process must be corrected immediately. In addition, Parenta management must be advised of the deviations and must initiate an investigation of the deviations (including the review of system activity log records, if necessary).

If the deviations identify a serious security problem (e.g., actual or attempted fraud or system compromise by an unauthorized individual or indication of misuse of authority), Parenta corporate security should be contacted.

Management must take appropriate action if a deviation is the result of authority misuse.

4 Reporting Security Incidents

A security incident can originate within or outside of Parenta, can involve other Parenta or external sites, and can range in severity.

Incidents involving violations of Parenta's Business Conduct Guidelines or Parenta's Internet Usage Guidelines can generally be referred to site management and personnel for resolution.

However, if any security incident potentially involves system penetrations, destruction or loss of data, fraud, crime or other serious matter, then adherence to the following methodology must be employed.

Upon incident discovery or being notified of a suspected incident, management must:

- If the suspected incident involves an Internet service, notify your Internet Service Provider.
- If the suspected incident does not involve an Internet service, as soon as it has been confirmed that an incident has occurred, notify Parenta’s corporate security providing:
    1. The management and technical contact points, phone numbers, and internal E-mail addresses
    2. A description of the problem, the extent to which the systems or data were compromised, the actions taken so far, and the system and network addresses involved.
- Immediately start a log file (on paper or on another system) to identify every piece of information related to the event. Include date and time and information source for each entry.

Corporate Security will provide instructions on how to proceed with the investigation.

- Do not attempt to perform the investigation on your own. You could unintentionally compromise the investigation or contaminate evidence.
- Do not contact individuals or organizations that you suspect of being the source of the incident.
- Do not try to reverse penetrate the origin of a system penetration attack. Attempting to do so could be illegal.
- Do not attempt to "clean up" the. A key aspect of incident investigation is preservation of evidence.

Information about these investigations is on a strict "need to know" basis. Therefore, do not disclose the investigation, its purpose, details, or findings to anyone inside Parenta. Unless directed by Parenta Legal counsel or Parenta executives, do not disclose investigation information to anyone outside of Parenta.

5 Legal requirements

5.1 Software Licenses:

All software resident on Parenta systems or servers must have a valid license.

Software should never be copied or duplicated, except as explicitly allowed in the license terms and conditions.

5.2 Export/Import Regulations:

Many countries impose strict regulations on exporting or importing advanced technology information. Advice should be sought from the relevant governing body if there is any uncertainty about importing or exporting any technology, software or any other asset.

6 Data Protection Act

The Data Protection Act 1998 was implemented and introduced in October 1998 as a result of European legislation to protect the rights and freedoms of individuals. It is intended to control and protect personal information held both on computer systems and in printed format. There are eight principles, which cover the issues within the Data Protection Act, and these are listed below.

- Process information fairly and lawfully treating sensitive data with extra care
- Only use the information for the purpose it was collected
- Ensure the information is adequate, relevant and not excessive for the purpose
- Keep information accurate and up to date
- Do not keep information for longer than is necessary
- Process information in accordance with the individuals rights
- Keep Data secure
- Ensure that adequate protection of information is provided before making transfers of Data outside the European Economic Area

All confidential information must be disposed of securely. In the case of printed material, this must be shredded, in the case of Computer Data a secure ‘wipe’ program should be used with Data being overwritten at least seven times.

7 The Internet

The use of the phrase ‘The Internet’ is a generic term that covers e-mail, File Transfer Protocol (FTP) and the World Wide Web (WWW) services among others.

7.1 Electronic Mail

Listed below are guidelines on the use of electronic mail:

- Distribution lists should be used cautiously. Electronic mail messages should be sent only to recipients who need the information. Automatic copying to all recipients of the original message should be avoided.
- Be succinct. The most effective e-mail messages are short and to the point.
- A subject line that captures the content of the message should always be used. This helps the recipients to priorities and search for messages. Some electronic mail systems will block messages that do not have a subject line.
- Electronic mails should only be sent to the classification approved for your system. Ensure messages have the appropriate security markings at the top of the message and on attachments.
- Messages should be tagged appropriately – do not label messages “immediate” or “high priority” unless they really are.
- An attachment size should be set with care: there may be size constraints at the recipient’s end.
- All electronic mail should be courteous and polite. Though by convention e-mail is less formal than conventional business correspondence, there is no place for inappropriate language.

7.2 Internet Usage - General

Parenta expressly forbids its staff from using the Internet to:

- Send junk e-mail, including lists of jokes
- Use profanities
- Use racial, sexual or defamatory remarks
- Send, or seek access to, or store pornographic or offensive material on any computer system or any other material, which is illegal, and or in contravention with the Laws of the Land. This can be a criminal offence and lead to instant dismissal and criminal prosecution.

The downloading of file(s) from the Internet contains an inherent risk, viruses, Trojan software or pirated version of commercial software to name a few. The following guidelines must be adhered too when using the Internet:

- Most information and software that is accessible on the Internet is subject to copyright or other intellectual property right protection. Therefore, nothing should be copied or downloaded from the Internet for use within Parenta unless express permission to do so is stated by the material owner.
- Materials distributed over the Internet in the form of "shareware" or "freeware", often come with express requirements or limitations attached (e.g., not to be used for commercial purposes; can not charge others for use or distribution; subject to a copyright or attribution notice being affixed to each copy, must distribute source code, etc.) If there are such terms applied, these must read and understood before downloading the software. A copy of the terms must be made if possible. If Parenta will not be able to comply with any part of the terms, the material should not be downloaded.
- Parenta employees&/or contractors must seek assistance and approval from the relevant Manager before incorporating anything downloaded from the Internet (or any external online service) into a product or material Parenta intends to distribute externally.
- Parenta Employees&/or contractors must not originate, forward or transmit any Parenta Client Data to any 3rd Parties via the Email system without approval/permission from IT Directors.

8 Back-up Procedure

Parenta has a back-up policy which all IT users should be aware of and adhere to.

All data located on Parenta servers or systems must be backed up on a daily basis.

Any data or documentation stored local on a User(s) own computer system (Hard Disk) will not be backed up by the system and it will be the responsibility of that user to recover and or replace any such Data that is lost.

Data backup media must be labelled properly and protected against unauthorized access (i.e., stored in a locked area or cabinet).

All backup procedures should have a reporting capability to advise of any failures via

- Log files that can be manually inspection
- or automated email notification,
- setting up and maintaining and monitoring the backup procedure are the system administrator's responsibility.

All backup strategies need to be subject to an annual review to ensure all required data has been backed up properly.

All server and system data backups are the responsibility of the storage media custodian

9 Windows Servers

Windows servers should be protected from unauthorized access by restricting them to be installed in CA(2) locations.

Windows servers should be rack mounted within cabinets where possible.

9.1 Boot Devices

To ensure only authorized methods of system booting are possible the first and only boot devices configured within BIOS should be the hard drive. Floppy drives, CD/DVD drives, network devices should be disabled from booting.

9.2 BIOS

System BIOS should be password protected and managed by either the system or network administrator.

9.3 USB Sticks

USB memory sticks should not be used and should be disabled through either the operating system in use or the system BIOS.

9.4 Removable Media

To ensure only authorized methods of data removal are possible any removable media should be disabled.

9.5 CD/DVD Writers

CD/DVD writers should be used for only reading media and not writing it. The ability to write media should be disabled through either the operating system in use or the system BIOS.

10 Unix Servers

This applies to any servers that have a Unix or Unix pedigree Operating Systems either bootstrapped or embedded.

Unix servers should be protected from unauthorized access by restricting to be installed in CA(2) locations.

Unix servers should be rack mounted within cabinets where possible.

10.1 Boot Devices

To ensure only authorized methods of system booting are possible the first and only boot devices configured within BIOS should be the hard drive. Floppy drives, CD/DVD drives, network devices should be disabled from booting.

10.2 BIOS

System BIOS should be password protected and managed by either the system or network administrator.

10.3 Removable Media

To ensure only authorized methods of data removal are possible any removable media should be disabled.

10.4 CD/DVD Writers

CD/DVD writers should be used for only reading media and not writing it. The ability to write media should be disabled through either the operating system in use or the system BIOS.

11 Desktop Systems

Desktop computer systems should be protected from unauthorized access by restricting access to removable media.

In order to only permit movement of data through managed and audited methods the following steps should be taken on all desktop systems and systems used by staff.

11.1 Boot Devices

To ensure only authorized methods of system booting are possible the first and only boot devices configured within BIOS should be the hard drive. Floppy drives, CD/DVD drives, network devices should be disabled from booting.

11.2 BIOS

System BIOS should be password protected and managed by either the system or network administrator.

11.3 Removable Media

To ensure only authorized methods of data removal are possible any removable media should be disabled.

11.4 CD/DVD Writers

CD/DVD writers should be used for only reading media and not writing it. The ability to write media should be disabled through either the operating system in use or the system BIOS.

11.5 USB Sticks

USB memory sticks should not be used and should be disabled through either the operating system in use or the system BIOS.

11.6 Mobile Communications

To ensure only authorized network connection methods are possible any wire free communication device or protocol should be disabled

11.6.1. InfraRed

IR devices should be disabled through either the operating system in use or the system BIOS

11.6.2. Bluetooth

Bluetooth devices should be disabled through either the operating system in use or the system BIOS

11.6.3. Wireless

Wireless network devices should be disabled through either the operating system in use or the system BIOS

11.6.4 Cameras and Camera Phones

These are not to be used to capture any information pertaining to any Data Classification within Parenta's Domain.

12 Laptop Systems

Due to the movement of laptop computers outside of Parenta buildings laptop computers should be configured to protect the data stored on them differently to that of desktop systems.

Laptop computers should be protected by, as a minimum, boot protection and disk and data encryption.

12.1 Boot Protection

Laptop computers should be configured to use an operating system boot protection method. This method should implement a logon inductor to exponentially increase the amount of time between sign on screens.

12.2 Disk Encryption

Laptop computers holding Parenta Client data should be protected by encrypting the entire hard drive with a sufficiently strong encryption algorithm. This method should be integrated with the boot protection to ensure authorized users have a user friendly method of access but unauthorized users are not able to either gain access or read any data if the hard drive was removed.

12.3 Data Encryption

Laptop users should encrypt critical files as per section 2.2.5

12.4 Mobile Communications

To ensure only authorized network connection methods are possible any wire free communication device or protocol should be disabled

12.4.1. InfraRed

IR devices should be disabled through either the operating system in use or the system BIOS

12.4.2. Bluetooth

Bluetooth devices should be disabled through either the operating system in use or the system BIOS

12.4.3. Wireless

Wireless network devices should be disabled through either the operating system in use or the system BIOS

13 Destruction of Old Systems

Any computer system that is deemed old and no longer required by Parenta should be subjected to the data destruction procedures.

13.1 Hard Drives

All hard drives should be removed from the original computer and be securely wiped using an approved method.

13.2 Removable Media

CD/DVD media, floppy disks, ZIP drives and other types of removable media containing Parenta data should be destroyed either by removing the external hard casing of the media and putting data element through a shredder or by burning.

13.3 Secure Wiping of Hard Drive

Hard drives to be re-used or are to leave Parenta's control should be securely erased using an approved wiping tool which should comply with the following:

- A pass of 7 times extended character rotation (US DoD 5200.28-STD)
- Over write with 1's
- Over write with 0's
- Over write with random

13.4 Secure Wiping of Files

Sensitive files that are to be deleted should also be done so using an approved wiping tool which should comply with:

- A pass of 7 times extended character rotation (US DoD 5200.28-STD)
- Wipe of swap file
- Wipe of directory entry