Juvenile Welfare Board
The Children's Services Council
of Pinellas County

Board of Directors Meeting
November 13, 2008

Information Technology Policies

Item V.C

Recommended Action: **Discussion Item**

Issue: **JWB needs to rewrite the Information Technology Policies to reflect changes in resources, business processes, and technology**.

Background:

Attached for discussion in November and action in December, is a summary of the JWB Technology Policies and Procedures which represents a major rewrite and reformatting to meet current industry standards. The full document contains both policy statements and detailed implementation guidelines, with Board approval requested for the policy statements. The Executive Director has the authority to approve any substantive changes to the guidelines, which can change more frequently. The complete text of the Policies is 288 pages and includes the detailed guidelines by which staff is to implement the policies presented to the Board for consideration. Staff will be receiving a handbook summarizing their responsibilities related to the use of technology at JWB.

Technology Policies are the means by which JWB establishes procedures to protect the investment made in technology. Information is a valuable asset that must be protected from unauthorized disclosure, modification, use or destruction. These policies represent prudent steps to ensure that its confidentiality, integrity and availability are not compromised. These policies are supported by continuous training of staff and monitoring of the network.

This document provides a uniform set of Information Technology Policies for using JWB Children Services Council of Pinellas County technology resources and all JWB Departments are required to abide by the policies. All users (employees, contractors, vendors, and other third parties) are expected to understand and abide by these policies. Staff will be provided training on these documents and all new employees will be required to be trained at orientation.

JWB Information Technology Policies are based upon the internationally recognized International Standard ISO/IEC 17799:2005 security standard framework. The policies are designed to comply with applicable laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security rules. In addition, recommendations from the annual audit and the SAS 70 conducted in September 2007 have been included. The recommendations for annual and quarterly security audits are also incorporated in this document.

This document was reviewed by DSM, Inc., the consulting firm that conducts the JWB's quarterly security audits. The review stated that: "…JWB made huge strides towards a complete set of security policies. The policies are adequate for an organization the size of JWB and should pass any associated audits."

Authority

The JWB IT Director is responsible for presenting recommendations to the Executive Director. The policies are to be reviewed quarterly with revisions submitted for Board approval at least every two years.

Volume 1

Information Technology Board Policies

ISO/IEC 17799

Prepared By:

Patricia K. Gehant, Director of Technology

JWB Children's Services Council of Pinellas County

September 2008

4 Risk Assessment and Treatment

4.1 Assessing security risks

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to JWB. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of JWB information systems.

JWB routinely conducts security audits of the networks and the JWB infrastructure. These reviews include social engineering tests of the workforce and brut force attempts to access the building. Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A social engineer runs what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security.

Security audits test the network configurations and security policies in place by both a review and scanning network access points for weaknesses. Issues are provided to staff for remediation.

4.2 Treating security risks

Before considering the treatment of a risk, JWB should decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for JWB. Such decisions should be recorded.

For each of the risks identified following the risk assessment a risk treatment decision needs to be made. Possible options for risk treatment include:

a) applying appropriate controls to reduce the risks;

b) knowingly and objectively accepting risks, providing they clearly satisfy JWB's policy and criteria for risk acceptance;

c) avoiding risks by not allowing actions that would cause the risks to occur;

d) transferring the associated risks to other parties, e.g. insurers or suppliers.

For those risks where the risk treatment decision has been to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by a risk assessment. Controls should ensure that risks are reduced to an acceptable level taking into account:

a) requirements and constraints of national and state legislation and regulations;
b) JWB objectives;
c) operational requirements and constraints;
d) cost of implementation and operation in relation to the risks being reduced, and remaining proportional to JWB's requirements and constraints;
e) the need to balance the investment in implementation and operation of controls against the harm likely to result from security failures.

JWB has selected controls from established standards, or from statutorily mandated controls for data protection and availability, previous audits including the SAS 70.

JWB considers ***Information security controls at the systems and projects requirements specification and design stage.***

This document represents the guidelines followed by all parties in the provision of technology for the purpose of conducting business.

5 Security Policy

5.1 Information Security Policy

Objective: To provide management direction and support for information security.

DISCUSSION - A clear policy direction must be established by the Board and management of JWB including the demonstration of support for, and commitment to, information security through the issue, maintenance, and enforcement of an information security policy across JWB.

5.1.1 Information Security Policy Document

Policy: An information security policy document will be approved by the Board and management, and published and communicated to all employees and relevant external parties at least every two years.

5.1.2 Review of the Information Security Policy

Policy: The review of the information security policies is the responsibility of the Director of Information Technology and should be reviewed every two years or when significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

6 Organization of Information Security

6.1 Information Security Infrastructure

Objective: To manage information security within the organization.

DISCUSSION: A management framework should be established to initiate and control the implementation of information security within the organization. Management should approve the information security procedures, assign security roles and co-ordinate and review the implementation of security across the organization.

6.1.1 Management Commitment to Information Security

Policy: Management should actively support security within JWB through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

6.1.2 Information Security Co-ordination

Policy: Information security policies should be coordinated throughout JWB by representatives on a team from different departments of JWB.

6.1.3 Allocation of Information Security Responsibilities

Policy: The Department Director is responsible for assuring that contactors/subcontractors and staff assigned to the division or department are in compliance with the security policies.

6.1.4 Confidentiality Agreements

Policy: All staff accessing the JWB network resources will annually sign a confidentiality or non-disclosure agreements reflecting JWB's needs for the protection of information annually.

6.1.5 Confidentiality Agreements

Policy: Third-party vendors, contractors and guests accessing the JWB network resources will sign a contract defining the terms and conditions before access are provided. A responsible manager or principal of the third-party organization and a JWB manager supervising the activities of the vendor, contractor, or guest must sign the contract.

6.1.6 Contact with Authorities

Policy: The IT department will maintain a list of appropriate contacts with relevant authorities or business partners to allow responsible staff to respond appropriately to security or network incidences that could impact the continuity of business.

6.1.7 Contact with Special Interest Groups

Policy: Appropriate contacts with special interest groups or other specialized security forums and professional associations should be maintained.

6.1.8 Independent Review of Information Security

Policy: JWB's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

6.2 External Parties

Objective: To maintain the security of JWB's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

DISCUSSION: The security of JWB's information and information processing facilities should not be reduced by the introduction of external party products or services.

Any access to JWB's information processing facilities and processing and communication of information by external parties should be controlled. Where there is a business need for working with external parties that may require access to JWB's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

6.2.1 Identification of Risks Related to External Parties

Policy: The risks to JWB's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

6.2.2 Addressing Security when dealing with Customers

Policy: All identified security requirements should be addressed before giving customers access to JWB's information or assets.

6.2.3 Addressing Security in Third Party Agreements

Policy: Agreements with third parties involving accessing, processing, communicating or managing JWB's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

7 Asset Management

7.1 Responsibility for Assets

Objective: To achieve and maintain appropriate protection of JWB assets.

All assets should be accounted for and have a nominated custodian.

Custodians should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned.

7.1.1 Inventory of Assets

Policy: All assets should be clearly identified and an inventory of all important assets drawn up and maintained in accordance with the financial policies of JWB.

7.1.2 Acceptable Use of Assets

Policy: JWB information technology resources are provided to authorize users to facilitate the efficient and effective performance of their duties in a secure electronic environment. The use of such resources imposes certain responsibilities and obligations on users and is subject to JWB policies. Rules for the acceptable use of information and assets associated with JWB should be identified, documented, and implemented.

7.2 Information Classification

Objective: To ensure that information receives an appropriate level of protection.

Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

7.2.1 Classification Guidelines

Policy: Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to JWB and in accordance with Florida Public Records Law, Chapter 119. FSS; and FSS 163.62 Section 1 Part 16.

7.2.2 Information Labeling and Handling

Policy: An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by JWB.

8 Human Resources Security

8.1 Prior to Employment

<u>Objective</u>: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Security responsibilities should be addressed prior to employment in job descriptions and in terms and conditions of employment.
All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

8.1.1 Roles and Responsibilities

<u>Policy</u>: Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with JWB's information security policy.

8.1.2 Screening

<u>Policy</u>: Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 Terms and Conditions of Employment

<u>Policy</u>: As part of their conditions of employment or contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions which should state the contractor's, third party vendor's and JWB's responsibilities for information security.

8.2 During Employment

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization.

An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third party users to minimize possible security risks. A formal disciplinary process for handling security breaches should be established.

8.2.1 Management Responsibilities

Policy: Management should require employees, contractors and third-party users to follow security guidelines in accordance with established policies and procedures of JWB.

8.2.2 Information Security Awareness, Education and Training

Policy: All employees of JWB and, where relevant, contractors and third-party users should receive appropriate awareness training and regular updates in JWB's policies and procedures, as relevant for their job function.

8.2.3 Disciplinary Process

Policy: Employees who have committed a security breach will be disciplined in accordance with the JWB HR Policies and Procedures. Contractors and third Parties will be disciplined in accordance with the contract.

8.3 Termination or Change of Employment

Objective: To ensure that employees, contractors and third party users exit JWB or change employment in an orderly manner.

Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from JWB is managed, and that the return of all equipment and the removal of all access rights are completed.

Change of responsibilities and employment within JWB should be managed as the termination of the respective responsibility or employment in line with this section, and any new employment should be managed as described in section 8.1.

8.3.1 Termination Responsibilities

Policy: Responsibilities for performing employment termination or change of employment are defined in the JWB HR Policies and Procedures.

8.3.2 Return of Assets

Policy: All employees, contractors and third party users are required to return all of JWB's assets in their possession upon termination of their employment, contract or agreement.

8.3.3 Removal of Access Rights

Policy: The access rights of all employees, contractors and third-party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

9 Physical and Environmental Security

9.1 Secure Areas

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

The protection provided should be commensurate with the identified risks.

9.1.1 Physical Security Perimeter

Policy: JWB will maintain the information systems in secure premises.

9.1.2 Physical Entry Controls

Policy: Entry controls will be placed on all exterior and interior doors to ensure that only authorized personnel are allowed access to area housing JWB information systems.

9.1.3 Protecting Against External and Environmental Threats

Policy: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

9.1.4 Working in Secure Areas

Policy: The areas housing information systems will be protected by applying and enforcing guidelines for working in secure areas.

9.1.5 Public Access, Delivery and Loading Areas

Policy: Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

9.2 Equipment Security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment location and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

9.2.1 Protection and Placement of Equipment

Policy: Equipment should be located in an appropriate location to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

9.2.2 Protection and Placement of Equipment– Desktops and Laptops

Policy: Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including personnel and client information, and that access to sensitive information is restricted to authorized users.

9.2.3 Protection and Placement of Equipment – Servers

Policy: Servers will be configured, monitored and secured from internal and external threats and unauthorized access.

9.2.4 Protection and Placement of Equipment – Virtual Private Networks (VPN)

Policy: Approved JWB employees and authorized third parties (customers, 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. Further details may be found in the Remote Access Policy.

9.2.5 Protection and Placement of Equipment – Internet DMZ Equipment

Policy: Equipment residing on the DMZ will be configured, monitored and secured from internal and external threats and unauthorized access.

9.2.6 Protection and Placement of Equipment – Internal Labs

Policy: This policy establishes information security requirements for JWB computer labs to ensure that JWB confidential information and technologies are not compromised, and that production services and other JWB interests are protected from lab activities.

9.2.7 Protection and Placement of Equipment – Routers

Policy: Every router connected to the JWB Network must meet the configuration standards that support the security policies in this document and established by the JWB Information Technology Department.

9.2.8 Protection and Placement of Equipment – Blackberry Communication Devices

Policy: JWB staffs are responsible for protecting all communication devices owned by JWB while assigned to or in their possession.

9.2.9 Supporting Utilities

Policy: Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

9.2.10 Cabling Security

Policy: Network, power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

9.2.11 Equipment Maintenance

Policy: All network equipment maintenance will be completed according to industry standards and recorded in the established IT tracking software to ensure its continued availability and integrity.

9.2.12 Securing of Equipment Off-Premises

Policy: JWB equipment located off site must be secured from unauthorized access and meet the security standards set forth in this document.

9.2.13 Secure Disposal or Re-use of Equipment

Policy: All items of equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

9.2.14 Removal of Property

Policy: Equipment, information or software should not be taken off-site without prior authorization.

9.2.15 Virus Protection

Policy: The virus protection software will be enabled on all network resources.

.

10 Communications and Operations Management

10.1 Operational Procedures and Responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures.

Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

10.1.1 Documented Operating Procedures

<u>Policy</u>: Operating procedures will be documented, maintained, and made available to all users as needed.

10.1.2 Change Management

<u>Policy</u>: Standardized methods and procedures will be implemented that are used for efficient and prompt handling of all changes to controlled IT infrastructure, in order to minimize the number and impact of any related incidents upon service.

10.1.3 Release Management

<u>Policy</u>: A process for release management will be developed to protect and preserve the quality of the live or production environment and its services through the use of formal procedures and checks before the change is introduced into the JWB information system environment.

10.1.4 Segregation of Duties

<u>Policy</u>: Duties and areas of responsibility within the IT department will be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of JWB's network resources.

10.1.5 Separation of Development, Test and Operational Facilities

<u>Policy</u>:

Controls should be instituted the provide reasonable assurance that implementations and changes to existing systems, and system software are authorized, tested, approved, and documented.

10.2 Third Party Service Delivery Management

<u>Objective</u>: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The organization will monitor and check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party. All agreements must comply with existing JWB Fiscal management policies.

10.2.1 Service Delivery

Policy: Controls should provide reasonable assurance that third-party services are defined appropriately and security requirements are clearly defined in performance contracts.

10.2.2 Monitoring and Review of Third Party Services

Policy: All contractor and third-party vendor agreements will be monitored and reviewed regularly.

10.3 System Planning and Acceptance

Objective: To minimize the risk of systems failures.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements should be made to reduce the risk of system overload.

The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

10.3.1 Capacity Management

Policy: The network and communication resources will be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

10.3.2 System Acceptance

Policy: Acceptance criteria for new information systems, upgrades, and new versions will be established and suitable tests of the system(s) will be carried out during development and prior to acceptance.

10.4 Protection against Malicious Software and Mobile Code

Objective: To protect the integrity of systems, software and information.

Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

10.4.1 Controls Against Malicious Software

Policy: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures are updated annually.

10.4.2 Controls Against Mobile Code

Policy: The configuration of mobile code will ensure that the authorized mobile code operates as intended, and network policies are configured to prevent any unauthorized mobile code from being executed.

10.5 Back-up

Objective:

To maintain the integrity and availability of information and information processing facilities.

Routine procedures should be established to implement the appropriate back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.

10.5.1 Information Back-up

Policy: Controls should provide reasonable assurance that the computer network resources are backed up on a periodic basis and procedures are employed to maintain the integrity of data. A test will be conducted at least annually of mission critical systems.

10.6 Network Security Management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

The secure management of networks, which may span organizational boundaries, requires careful consideration of data flow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

10.6.1 Network Controls

<u>Policy</u>: The JWB Network will be managed and controlled, in order to protect it from threats, and to maintain security for the systems and applications using the network, including the transit of information.

10.6.2 Security of Network Services

<u>Policy</u>: Security features, service levels, and management requirements of all network services will be provided to all users, contractors and third party vendors for all network services agreements, whether these services are provided in-house or outsourced.

10.7 Media Handling

<u>Objective</u>: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

Media should be controlled and physically protected.
Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks, jump devices, flash drives, CD's), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

10.7.1 Management of Removable Media

<u>Policy</u>: This policy addresses the requirement for the proper security, handling, and disposal of JWB information contained in removable media.

10.7.2 Disposal of Media

<u>Policy</u>: All data storage devices will be assessed by Information Technology Department prior to the distribution outside of JWB, disposal or destruction.

10.7.3 Information Handling Procedures

<u>Policy</u>: Staff will follow JWB or third party published procedures for the handling and storage of information stored on the JWB Network or any equipment owned or operated by JWB employees in order to protect this information from unauthorized disclosure or misuse.

10.7.4 Security of System Documentation

Policy: System documentation will be stored in a locked facility and protected against unauthorized access.

10.8 Exchange of Information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

Exchanges of information and software between organizations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation.

Procedures and standards should be established to protect information and physical media containing information in transit.

10.8.1 Information Exchange Policies and Procedures

Policy: Data exchange policies, procedures, and controls will be in place for all systems that contain client identifying data and will describe the limitations of use, access rights, and distribution standards.

10.8.2 Exchange Agreements

Policy: Agreements should be established for the exchange of information and software between JWB and external parties.

10.8.3 Physical Media in Transit

Policy: Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond JWB's physical boundaries.

10.8.4 Electronic Messaging

Policy: Information contained in electronic messages will be protected.

10.8.5 Business Information Systems

Policy: Interconnected business systems will be reviewed to determine the appropriateness of the connection on a regular basis.

10.9 Electronic Commerce Services

Objective: To ensure the security of electronic commerce services, and their secure use.

The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, should be considered. The integrity and availability of information electronically published through publicly available systems should also be considered.

10.9.1 Electronic Commerce

Policy: Information involved in electronic commerce passing over public networks will be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

10.9.2 On-line Transactions

Policy*:* Information involved in on-line transactions will be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

10.9.3 Database Management

Policy*:* Databases will be protected from unauthorized access and malicious damage.

10.10 Monitoring

Objective: To detect unauthorized information processing activities.

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.

10.10.1 Audit Logging

Policy: Audit logs recording user activities, exceptions, and information security events are produced and kept for up to one year to assist in future investigations and access control monitoring.

10.10.2 Monitoring System Use

Policy: The JWB Network will be monitored for use and the results of the monitoring activities reviewed regularly.

10.10.3 Protection of Log Information

Policy: Logging facilities and log information will be protected against tampering and unauthorized access.

10.10.4 Administrator and Operator Logs

Policy: System administrator and system operator activities will be logged for all mission critical and sensitive business system.

10.10.5 Fault Logging

Policy: Faults will be logged, analyzed, and appropriate action taken.

10.10.6 Clock Synchronization

Policy: The system clocks of all relevant information processing systems (servers) within the JWB network will be synchronized twice a year.

11 Access Control

11.1 Business Requirement for Access Control

Objective: To control access to information.

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

Access control rules should take account of policies for information dissemination and authorization.

11.1.1 Access Control Policy

Policy: Access to JWB network and desktop resources will be based on documented business and security requirements.

11.2 User Access Management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

Formal procedures are in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

11.2.1 User Registration

Policy: User registration and de-registration procedures will be enforced for granting and revoking access to all information systems and services.

11.2.2 User Registration – SAMIS

Policy: To inform all SAMIS users of responsibility for granting and revoking access to SAMIS.

11.2.3 User Registration – KnowledgeShare

Policy: KnowledgeShare accounts are issued to grant access to JWB's KnowledgeShare Portal and users will conform to all User Registration policies.

11.2.4 Privilege Management

Policy: Access to network and multi user systems will be based on a formal and documented process managed by the Information Technology Department based on the IT Policies and Procedures.

11.2.5 User Password Management

Policy: The allocation of passwords shall be controlled through a formal management process.

11.2.6 Review of User Access Rights

Policy: Management will review and update all user access rights at least annually using a formal process.

11.3 User Responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

The co-operation of authorized users is essential for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. A clear desk and clear screen policy should be implemented to reduce the risk of unauthorized access or damage to papers, media, electronic data, and information processing equipment and facilities.

11.3.1 Password Use

Policy: All personnel who are granted a password are responsible for managing the account in accordance with password guidelines.

11.3.2 Unattended User Equipment

Policy: Users are responsible for securing unattended equipment appropriately to ensure its protection and safety.

11.3.3 Clear Desk and Clear Screen Policy

Policy: The clear desk policy for papers and removable storage media and a clear screen policy for staff will be implemented for persons with access to sensitive information. See 7.1.2

11.3.4 Workstation Policy

Policy: Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI), client information, and that access to sensitive information is restricted to authorized users.

11.3.5 Acceptable Use

Policy: All persons granted access to the JWB network and equipment will adhere to the Acceptable Use Policy.

11.3.6 Acceptable Use KnowledgeShare (SharePoint)

Policy: Users must not attempt to access any data or programs contained on JWB KnowledgeShare property for which they do not have authorization or explicit consent.

11.3.7 Acceptable Use – Email Communication

Policy: Personnel granted access to JWB email will adhere to the guidelines for use of email.

11.4 Network Services

11.4.1 Policy on Use of Network Services

Policy: Users should only be provided with access to the network services that they have been specifically authorized to use.

11.4.2 User Authentication for External Connections

Policy: Mobile computing and storage devices containing or accessing the information resources at JWB must be approved prior to connecting to the information systems at the JWB. This pertains to all devices connecting to the network at JWB, regardless of ownership.

11.4.3 Equipment Identification in Networks

Policy: Automatic equipment identification procedures will be in place as a means to authenticate connections from specific locations and equipment.

11.5 Operating System Access Control

Objective: To prevent unauthorized access to operating systems.

Secure facilities should restrict access to operating systems to authorized users only. The facilities should be capable of the following:

- Authenticating authorized users, in accordance with a defined access control policy;
- recording successful and failed system authentication attempts;
- recording the use of special system privileges;
- issuing alarms when system security policies are breached;
- providing appropriate means for authentication;
- where appropriate, restricting the connection time of users.

11.5.1 Secure Log-on Procedures

Policy: Access to operating systems is limited to designated IT staff.

11.6 Mobile Computing and Telecommuting

Objective: To ensure information security when using mobile computing and telecommuting facilities.

The protection required should be commensurate with the risks. When using mobile computing, the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of telecommuting the organization should apply protection to the telecommuting site and ensure that suitable arrangements are in place.

11.6.1 Telecommuting

Policy: A policy, operational plans and procedures will be developed and implemented for telecommuting activities.

12 Information Systems Acquisition, Development, and Maintenance

12.1 Security Requirements of Information Systems

Objective: To ensure that security is an integral part of information systems.

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

12.1.1 Security Requirements Analysis and Specification

Policy: A statement of business requirements for new information systems, or enhancements to existing information systems should follow a standard Software Development Life Cycle Design process and incorporate security requirements, analysis and specifications of JWB.

12.1.2 Access Control to Program Source Code

Policy: Access to program source code is restricted to qualified staff and approved vendors.

12.1.3 Outsourced Software Development

Policy: Outsourced software development will be supervised and meet the standards for development set forth by JWB.

13 Compliance

13.1 Compliance with Legal Requirements

Objective: To avoid breaches of any law, statute, regulation or contractual obligation, and of any security requirements.

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from JWB's legal advisers. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e., Trans-border data flow).

13.1.1 Identification of Applicable Legislation

Policy: All relevant statutory, regulatory, and contractual requirements and JWB's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and JWB.