

SAGAMING

Information Security Policy

Revision	Date	Security Class	Purpose
1.0	March 13, 2025	Confidential	Creation and approval

Table of Content

1.	Purpose	5
2.	Scope	6
3.	Objective	6
4.	Using the Policies	7
5.	Roles and Responsibilities	8
5.1	Security Management Group	8
5.2	Directors, Managers and Leads	8
5.3	Information Owner	9
5.4	Information Users	10
6.	Information Security Policy	10
6.1	Organization of Information Security	11
6.1.1	Authorization Process for Information Processing Facilities.....	11
6.1.2	Confidentiality Agreements	11
6.1.3	External Parties	11
6.1.4	Contact with Authorities and Special Interest Groups	11
6.1.5	Independent Review of Information Security	11
6.2	Risk Assessment and Treatment.....	12
6.2.1	Assessing Security Risks.....	12
6.2.2	Treating Security Risks and Threats	12
6.2.3	Audit Logs	13
6.3	Asset Management	13
6.3.1	Information Classification	13
6.3.2	Classification Guidelines.....	14
6.3.3	Acceptable Use of Assets	14
6.4	Human Resources Security	14
6.4.1	Prior to Employment.....	14
6.4.2	Roles and Responsibilities.....	15
6.4.3	Screening.....	15
6.4.4	Terms and Conditions of Employment	15
6.4.5	Management Responsibilities	16
6.4.6	Information Security Awareness and Training	16
6.4.7	Disciplinary Process	16
6.4.8	Termination or Change of Employment.....	16

6.4.9	Termination Responsibilities.....	17
6.4.10	Return of Assets.....	17
6.4.11	Removal of Access Rights.....	17
6.5	Physical and Environment Security	17
6.5.1	Physical Security Perimeter and Entry Controls	17
6.5.2	Securing Offices, Rooms, and Facilities	18
6.5.3	Protecting Against External and Environmental Threats.....	18
6.5.4	Public Access, Delivery, and Loading Areas	18
6.5.5	Equipment and Cabling Security	19
6.5.6	Secure Disposal of Equipment	19
6.6	Communications and Operations Management	19
6.6.1	Documented Operating Procedures.....	19
6.6.2	Change Management.....	19
6.6.3	Segregation of Duties	20
6.6.4	Separation of Development, Test, and Operational Facilities	20
6.6.5	Third Party Service Delivery Management	21
6.6.6	Monitoring and Review of Third Party Services	21
6.6.7	Managing Changes to Third Party Service	21
6.6.8	System Planning and Acceptance	21
6.6.9	Capacity Management	22
6.6.10	Protection Against Malicious Code and Mobile Code	22
6.6.11	Back-Up	22
6.6.12	Network Security Management	22
6.6.13	Removal and Seizure	23
6.6.14	Media Handling	23
6.6.15	Exchange of Information	23
6.6.16	Physical Media in Transit	23
6.6.17	Electronic Messaging	24
6.6.18	Electronic Commerce Services	24
6.6.19	Monitoring	24
6.6.20	Clock synchronization	25
6.7	Access Control	25
6.7.1	User Access Control	25
6.7.2	Review of Access Rights	25
6.7.3	Unattended User Equipment	26

6.7.4	Clear Desk and Clear Screen Policy	26
6.7.5	Network Access Control	26
6.7.6	User Authentication of External Connections	26
6.7.7	Equipment Identification in Networks	26
6.7.8	Remote Diagnostic and Configuration of Protection	26
6.7.9	Segregation in Networks	26
6.7.10	Application and Operating System Access Control	27
6.7.11	Mobile Computing and Teleworking	27
6.8	Information Systems Acquisition, Development and Maintenance	28
6.8.1	Correct Processing in Applications	28
6.8.2	Use of Encryption	28
6.8.3	Security of System Files	28
6.8.4	Security in Development and Support Processes	28
6.8.5	Change Control Procedures	29
6.8.6	Restrictions on Changes to Software Packages	29
6.8.7	Outsourced Software Development	29
6.8.8	Technical Vulnerability Management	29
6.9	Information Security Incident Management	29
6.10	Business Continuity Management	31
6.10.1	Business Continuity and Risk assessment.....	31
6.10.2	Testing,Maintaining and Re-assessing Business Continuity Plans...	31
6.11	Information Systems Acquisition, Development and Maintenance	31
6.11.1	Privacy of Personal Information	31
6.11.2	Copyrights	32
6.11.3	Licensed Materials	32
6.11.4	Release of Corporate Information	32
6.11.5	Records Management	32
7.	Information Security Policy Exceptions	33

1. Purpose

SA Gaming Technology Limited ("SA GAMING") views all information resident in its various systems as a company asset. Information includes, but is not limited to: technical, financial, staffing, payroll, computer systems, marketing, advertising, merchandising, product, benefits, customer data, trade secrets, branding or other information similar to the aforementioned on paper, voice, electronic or any form.

Information security policies and related documents are created, developed and published as a means to implement SA GAMING's management intent, direction, and support for information security in accordance with SA GAMING's business requirements, operational and administrative functions, and relevant laws, regulations, and contractual agreements.

It is the intent of these documents, labeled as SA GAMING Information Security Policies, Standards, and Procedure, to supersede all other policies, guidelines, standards, and procedures.

It is vitally important to SA GAMING's reputation, operation and financial well being that information assets contain mechanisms to ensure the confidentiality, integrity and availability of resources owned and controlled by SA GAMING. These controls must protect the enterprise's information assets, and the business processes they support, against unauthorized use, disclosure, transfer, modifications or destruction, whether accidental or intentional, or the denial of availability of these assets or business processes to authorized users. In addition, legislative requirements governing the misuse of computers and the protection of personal data require a commitment to ensuring the security of those resources. Violations of these policies should be dealt with by Human Resources. Failure to comply with these policies may result in disciplinary action, up to and including termination of employment as well as civil and/or criminal actions.

This document establishes the basis of information security policies, related documents that establish criteria for access to, through or from SA GAMING's communication networks. The Information Security Policy is intended to establish the information security criteria, means, methods, and measures to protect the confidentiality, integrity, and availability of SA GAMING's information assets and communication networks. The policy will establish the rules for the access and use of data, information and the network infrastructure; and to mitigate the risks and losses associated with security threats to the networks, data assets, and information resources.

SA GAMING's approach to information security is a process. This process begins with strategic information security policies from SA GAMING's management. With the understanding that certain procedures are not currently in place to fully comply with these policies, it is intended that all reasonable efforts be made to bring such procedures into compliance with these documents. Until such time that these procedures are in compliance, SA GAMING should review these policies and develop appropriate projects to bring their systems into compliance.

2. Scope

The company is committed to protecting its information and that of its customers.

This policy applies to all SA GAMING employees, vendors and contractors who are granted access to all SA GAMING's corporate networks and system applications for the purpose of doing work with or for SA GAMING. This document references technical areas for the protection of the integrity, confidentiality and availability of SA GAMING's data and information whether it is processed, transmitted, stored on and/or in transit through SA GAMING networks, data system networks and networked computer systems.

This operational document is not intended to replace any policy contained in SA GAMING's employee handbook but rather to supplement the same and offer operational guidance. Interpretation and application of these procedures remains at all times within the discretion of SA GAMING. With the exception of employment at-will, all policies, terms and conditions of employment with the Company may be modified at the sole discretion of the company with or without cause or notice at any time.

3. Objective

It is the policy of our company to ensure:

- Information is only accessible to authorized persons from within or outside the company.
- Confidentiality of information is maintained.
- Integrity of information is maintained throughout the process.
- Business continuity plans are established, maintained, and tested.

- All personnel are trained on information security and are informed that compliance with the policy is mandatory.
- All breaches of information security and suspected weaknesses are reported and investigated.
- Procedures exist to support the policy, including virus control measures, passwords, and continuity plans.
- Business requirements for availability of information and systems will be met.
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

4. Using the Policies

The Information Security Policies are intended as a reference document to guide business units in developing procedures and processes in a consistent framework. The policies are supported by individual business unit procedures, practices, briefings, manager's guidelines and supporting awareness material that are made available to the business unit and others outside the business unit on a need-to-know basis.

In implementing the policies, business units will employ the following process:

- Review existing procedures and practices against the policies
- Document positions against the policies
- Perform a gap analysis to identify deficiencies
- Document deficiencies
- Document the group's plan to close identified gaps
- Document new business unit procedures and practices
- Determine the appropriate distribution or access for business unit procedures
- Allocate funds and resources towards closing identified gaps

In the case where a business unit has a regulatory requirement for increased security, or needs to have an exception to the corporate information security policy for a valid business reason, SA GAMING's management will review the request, including the business and

regulatory requirement that needs to be met, and will approve such requests on a case by case basis.

5. Roles and Responsibilities

All internal, remote systems, information assets, resources, and communication networks deployed at SA GAMING must be owned by an operational group that is responsible for its system and network administration. Ownership is to be designed by senior management. Approved configuration, processes, implementation and related documentation must be established and maintained by each operational group, based on business needs and approved by the Security Management Group.

5.1 Security Management Group

This group is responsible for ratification and enforcement of SA GAMING strategic direction, policy and oversight for information security.

5.2 Directors, Managers and Leads

Directors, Managers and Project Leads with responsibility for information assets must carry out all the appropriate responsibilities as a manager for their responsible area. In addition, they will act as the Custodian of information used by systems that they manage but which are owned by other managers. They must ensure that Information Owners are identified, appointed and made aware of their responsibilities.

All directors, managers and leads have an advisory and assisting role to SA GAMING information security in respect to:

- Identifying and assessing risks
- Identifying and implementing protective measures
- Maintaining a satisfactory level of security awareness
- Monitoring the proper operation of security measures within the business unit
- Investigating any weaknesses and occurrences
- Raising any new issues or circumstances of which they become aware

5.3 Information Owner

The Information Owner is a director or manager in an area that generates or processes an information asset (e.g. application programs and related files), or produces products and services that depend upon an information system. Each application and system must have an Information Owner responsible for its protection. This involves the authorization of user access to system information, the control of changes to system information, and the assurance that essential functions and those applications are recoverable in the event the existing environment becomes unavailable.

The director or manager must:

- Define appropriate requirements to ensure the availability, confidentiality and integrity of the information
- Identify and define the assets and security processes associated with individual systems, applications or processes that house the information
- Document the responsibilities of the system or application manager
- Establish the exact nature and extent of authorized access and use of information
- Specifically authorize individuals for access to information
- Ensure that accurate, up-to-date records are kept on access given
- Regularly check the continuing validity and proper operation of the protective measures and access authorities
- Ensure that all access is disabled and company-owned assets be returned upon employee termination
- Report occurrences that violate protective measures or threaten to cause an unacceptable risk
- Classify information in accordance with SA GAMING's Information Classification Standard
- Support and participate in investigations of incidents
- Responsible for providing Business Impact Assessment information

Applications that are cross functional in nature, in that they serve the needs of multiple groups, will have a central Information Owner who will serve as a focal point for management of access to the application. For enterprise system software, the Information Custodian of a computer system will serve as the Information Owner.

The director or manager will serve as the Information Owner of applications running on the group's personal computers, unless another Information Owner has been explicitly assigned. In each case, the Information Owner must designate in writing, a person as a back up, if the Information Owner should be unavailable.

5.4 Information Users

All internal and contract personnel using SA GAMING's information or systems must be personally aware of the Information Security Policies, Standards and Procedures.

Information users must:

- Ensure that appropriate authorization for access to information is acquired
- Comply with all relevant laws and regulations
- Comply with all applicable SA GAMING policies, standards and procedures
- Draw attention of management for any relevant issues, circumstances or weaknesses in SA GAMING's information security systems.

6. Information Security Policy

This document establishes the policies that institute the standards and procedures that are to be followed to assure that SA GAMING's information assets and resources, both technological and not, are appropriately protected when authorizing the access to networked information, assets and systems. The Information Security policy-related documentation should provide the details of the controls over what information assets are available such as to the following:

- Installed hardware, software and support contracts
- Implementation of security management (i.e. confidentiality and integrity mechanisms of transmitted and stored data)
- Access provision (i.e. system documentation of privileges assigned to remote users and clients)

6.1 Organization of Information Security

6.1.1 Authorization Process for Information Processing Facilities

A process for authorizing new information facilities should be defined and implemented. Facilities should have appropriate user management authorization, authorizing their purpose and use.

6.1.2 Confidentiality Agreements

Confidentiality or Non-Disclosure Agreements (NDA) reflecting the organization's needs for the protection of information should be identified and regularly reviewed.

All contracts must have an associated, valid NDA specific to the work being accomplished. SA GAMING must ensure all security requirements written into contractual agreements are followed by the partner.

6.1.3 External Parties

All third parties developing, accessing or using SA GAMING's information resources must be sponsored by a SA GAMING director level official. The risks to SA GAMING's information and processing facilities from business processes involving external parties should be identified and accepted by a SA GAMING management official prior to granting access.

6.1.4 Contact with Authorities and Special Interest Groups

Appropriate contact with authorities, special interest groups, or other specialist security forums and professional associations should be maintained. All contact with external groups should be sponsored and endorsed by a member of the SA GAMING management team.

6.1.5 Independent Review of Information Security

SA GAMING's approach to managing information security and its implementations (e.g. control objectives, policies, standards, processes) should have an independent review annually, or when significant changes to the security implementation occur.

6.2 Risk Assessment and Treatment

6.2.1 Assessing Security Risks

Risks to the corporate environment must be addressed on a proactive basis. Risks must be identified and decisions made to either develop control activities to mitigate the risks, accept the risks, or transfer the risks. Risk management is a joint effort between SA GAMING's Senior Management, Risk Management group and the IT Audit group.

The Risk Management group should be involved in assessing risk for the enterprise.

- During the development of new applications and systems
- When changing existing systems
- When business processes change
- When specific areas of concern are identified

All risk assessments must be documented.

The Risk Management group is responsible for the management of the residual risk associated with this policy. Risk management is focused on the following activities:

- Vulnerability awareness and management
- Threat awareness and management
- Risk assessment
- Audit controls
- Incident management and response
- Security awareness training
- Forensic investigations

6.2.2 Treating Security Risks and Threats

The Risk Management group must define and implement a program to maintain internal awareness of the evolution of vulnerabilities and the consequent implications of changes to the risk portfolio. Significant new vulnerability information must be routinely reported to senior management. Risk Management group must periodically conduct Vulnerability Assessments to ensure that the security policy continues to be effective in minimizing vulnerabilities in the operational environment.

The Risk Management group must define and implement a program to maintain internal awareness of the evolution of the current threats and the implications for changes to the

risk portfolio. Significant new threat information must be routinely reported to senior management.

6.2.3 Audit Logs

Audit trails enable recreation of chains of events and are very important in tracing activity during and after a risk or threat assessment. Security administrators must be provided with training in analysis of audit trails. The centralized audit system employed must be configured to produce a series of reports automatically. The reports must be reviewed on a regular and timely basis. Reporting must make use of an exception reporting process to ensure that the most important events are seen and investigated.

All logs relevant to risk and threat assessments must be archived with the Risk Management group for future reference noting the validity of identified risks and threats.

6.3 Asset Management

An accurate inventory of significant information assets must be maintained. All major resources must have a designated owner who is responsible for maintaining appropriate controls for assets. Implementation responsibilities may be delegated, but accountability remains with the assigned owner of the asset. All significant information resources must periodically be subject to inventorying.

Assets to inventory include hardware, software, contractual agreements for hardware, software purchases and licensing, service and maintenance contracts, outsourcing, external development, partner access, customer access and joint ventures.

An inventory accounting of these assets is to be maintained either physically or electronically and include the contract term, impact of loss and security classification.

A reconciliation of the information resources inventory must take place on a regular basis.

6.3.1 Information Classification

Information must be properly classified in order to ensure that information created or received in the course of business will not impair SA GAMING's legal, financial or competitive position or image, if disclosed outside SA GAMING without using appropriate restrictions. It is the responsibility of the business unit and individuals generating

information to classify the information and maintain a record of distributed information for sensitive information. These records must be reviewed annually. Each business unit must develop procedures for the proper classification, handling, reproducing, storing, disclosing and disposing of information regardless of its form (e.g. hard drive, back up tapes, paper).

The aggregation of data at a lower classification may be used to infer new information at a higher classification level. This situation must be considered when assigning an information classification.

If SA GAMING's sensitive information is accidentally disclosed to an unauthorized party, the individual discovering the compromise will immediately notify their management or report the incident to the Risk Management group.

6.3.2 Classification Guidelines

All information will receive at least one sensitivity level classification as defined by the Data Sensitivity Classification Standard. Information Owners will additionally classify any relevant information in accordance with the Data Functionality Classification Standard.

The classification standards and procedures for protecting, labeling and handling of information will be defined by both the Data Sensitivity Classification Standard and Data Functionality Classification Standard.

6.3.3 Acceptable Use of Assets

Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

6.4 Human Resources Security

6.4.1 Prior to Employment

To ensure employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, SA GAMING should perform adequate security screening prior to employment or engagement.

6.4.2 Roles and Responsibilities

Security roles and responsibilities should be documented where appropriate by managers and Human Resources. The roles should include any general responsibilities for implementing or maintaining security policies as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

6.4.3 Screening

Pre-hire screening must be performed for all employees, interns, and contractors prior to being granted access to SA GAMING's networks. Human Resources screening procedures must be followed. Personnel in charge of temporary or contract employees must contact Human Resources for advice on pre-contract screening.

Business to business pre-screening will be handled contractually prior to engagement to verify that the engaging company meets SA GAMING's minimum pre-screening procedures for their employees.

Additional screening may be required per job description and job location requirements. Personnel who access information processing facilities for sensitive information, e.g. financial, or other sensitive information (as defined in the Data Sensitivity Classification Standard] classified information are to have additional screening requirements.

For personnel holding positions of considerable authority, the screening process should be repeated periodically. Agencies responsible for providing contract personnel should include the aforementioned screening requirements. The communication of verifying actions are to include notification of any negative and incomplete check information to hiring management prior to personnel assignment.

6.4.4 Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors, and third party users should agree and sign the terms and conditions of their employment contract, which should state their responsibilities for information security.

Employees should sign a confidentiality and/or non-disclosure agreement as part of their initial terms and conditions of employment. Contract staff and third party users not already covered by an existing contract (containing the confidentiality agreement) should be

required to sign a confidentiality agreement prior to being given access to information processing facilities. Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

6.4.5 Management Responsibilities

SA GAMING management is responsible for requiring employees, contractors, and third party users to apply security in accordance with established policies, standards, and procedures of SA GAMING.

6.4.6 Information Security Awareness and Training

An information security awareness and training program for ALL SA GAMING employees, contractors, and third party users, is to be created, maintained, and reviewed annually by the Security Management Group.

This program must address professional training requirements for technology managers, security management, security administrators, programmers, and any other personnel requiring professional training to facilitate compliance with SA GAMING's security directive, policies, standards and system administration best practices.

All users of SA GAMING's information assets must be given Security Awareness Training that will detail the Users' responsibilities and address best practices for satisfying those responsibilities. The training should occur in new hire orientation, as well as annually. Upon completion of new-hire training, Users must sign an Acceptable Use Agreement indicating compliance. The Acceptable Use Agreement then becomes part of the users' permanent personnel file which resides with Human Resources.

6.4.7 Disciplinary Process

Managers must refer to their Human Resources representative for advice on handling non-compliance with SA GAMING's information security directive, policies, standards or procedures.

6.4.8 Termination or Change of Employment

To ensure protection of SA GAMING's information assets, procedures should be developed for removing access to SA GAMINGs systems and physical locations, as well as return of all

SA GAMING assets and information upon an employee's roles and responsibilities terminating or changing.

6.4.9 Termination Responsibilities

Responsibilities for performing termination or change of employment should be clearly defined and reviewed annually by Human Resources.

6.4.10 Return of Assets

All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

6.4.11 Removal of Access Rights

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.

6.5 Physical and Environment Security

6.5.1 Physical Security Perimeter and Entry Controls

All employees are responsible for protecting SA GAMING's information assets, employees, property, services, revenues, proprietary information and image from damage, theft, misuse, or unauthorized use. In an effort to fulfill this responsibility, only company employees or authorized agents are allowed unescorted access to company facilities.

Each facility must adhere to the established procedures for controlling building access. The following controls should be implemented as permitted by local law:

- Employees will be issued photographic identification badges that must be worn in a visible manner at all times, while the employee is in any company facility
- With proper authorization, photographic vendor identification badges may be issued to vendors, contractors, or others who are assigned to company facilities and report to work there on a daily basis for extended periods. Employee identification badges and vendor badges must be worn in a visible manner while in the barrier of the company facility that is not generally open to the public

- All other visitors must be signed in and escorted by a company employee throughout the time that the visitor is in a company facility
- All visitors should receive written and/or verbal instructions on the visited area's security requirements and emergency procedures
- Any employee who discovers an unauthorized individual within a company facility should ask that individual for identification, notify their supervisor, building security, or contact Security Management group
- Any packages, objects or bags brought into or removed from company facilities are subject to inspection
- Access rights to facilities must be regularly reviewed and updated
- Access rights to facilities must be removed upon employee/contractor termination or a change in job responsibilities that no longer require physical access to the facility

6.5.2 Securing Offices, Rooms, and Facilities

SA GAMING's information assets must be physically protected from damage, theft, interruptions to business processes, and health regulations. Critical business information processing facilities must be housed in secure areas, and be protected by a defined perimeter with appropriate security barriers and entry controls. All fire doors on the perimeter should have alarms and should close automatically. All areas of the facility should be protected by alarms. Facilities housing secure areas should be designed so as to give minimum indication of their purpose. The protection provided must commensurate with identified risks whether hosted locally or by a third party. Unsupervised work activity in secure areas is to be avoided both for personnel safety and to prevent opportunities for malicious actions. Physical access controls must include those that restrict and monitor entry to the data center, telecommunications network facility, or ancillary areas (e.g., generator or UPS storage rooms).

6.5.3 Protecting Against External and Environmental Threats

Physical protection against damage from fires, floods, earthquakes, explosions, civil unrest, and other forms of natural or manmade disasters should be designed and applied.

6.5.4 Public Access, Delivery, and Loading Areas

Access to receiving areas by delivery personnel should be restricted to identified and authorized personnel and delivery companies. The receiving area should be designed so that items can be unloaded without delivery staff gaining access to other parts of the

building. When possible, the external door(s) of a holding area should be secured when an internal door is opened. All incoming material should be inspected for potential hazards and logged before it's moved from the holding area to its point of use.

6.5.5 Equipment and Cabling Security

Equipment, including personal computing devices and portable or handheld devices must be physically protected from security threats, environmental hazards, and maintained according to manufacturer's specifications. Protection of equipment and information, including equipment located at off-site facilities, is required to reduce the risk of unauthorized access to data and to protect against loss or damage. Any equipment or media taken off-premises should not be left unattended in public areas. Lost or stolen computing devices must be reported immediately to the business unit management and Security Management group.

Electric and telecommunications cabling should also be segregated to avoid interference.

6.5.6 Secure Disposal of Equipment

Computers, storage components, removable storage media, and printed products that contain or have ever contained SA GAMING information must be disposed of in a secure manner.

6.6 Communications and Operations Management

6.6.1 Documented Operating Procedures

Daily operational procedures should be created, documented, maintained and tested. These procedures should be made available to all users who need them. All technology usage must follow explicit management approval.

6.6.2 Change Management

A change management review team composed of representatives from the development staff, computer operations, network management, information owners, physical facilities personnel, system users and Information Technology personnel must be instituted. The review team must prioritize all changes, schedule the changes for appropriate times to ensure a stable operating environment, and be responsible for communicating the planned

changes to the affected users and support personnel. Vulnerability assessment testing must be implemented as part of the change control process and be utilized when changes to networks, servers, applications, databases, routers and switches are implemented. All change control activity must account for time to back out the change if problems occur to ensure the change control window can accommodate all the scheduled activity.

6.6.3 Segregation of Duties

To prevent fraud and misuse, operational duties should be segregated so that no individual can avoid detection without collusion with another individual. In all cases, the rule of least privilege must be applied (i.e., users should be given the least amount of privileges required to carry out their job responsibilities).

For example, security administration functions must be segregated from the performance of other functions requiring a high degree of administrative privilege, control over the information resource being administered, or control over system or security administration software.

6.6.4 Separation of Development, Test, and Operational Facilities

Development and testing must be performed in an environment that is separated from production, either physically or logically, to ensure that testing and production processing cannot impact each other. If possible, testing should not involve any components of the production environment, including software, hardware, and network connectivity.

- The development environment must comply with all security policies, infrastructure standards, and procedures for production networks if it is to be installed on a production network.
- Testing should be done only with test data; production files and data must never be impacted by the development process.
- If access to production data is required, such access must be limited to read only.
- If production data is used for testing, it must be provided the same level of protection in a test environment as it receives in the production environment.
- If feasible, when using production data for testing, any critical or confidential data should be sanitized or deleted.
- Production processing must be performed only with production data. Production data must never be affected by the testing process.

- Development hardware must not be migrated to a production environment until all development and testing is completed. It is recommended that the operating system and all file systems be reinstalled and reinitialized to ensure that all production security controls are in place.

6.6.5 Third Party Service Delivery Management

SA GAMING's data and information assets must be consistently protected. Third party users using or having access to the organization's assets should be aware of the limits existing for their use of organization's information and assets associated with information processing facilities, and resources. Access, access rights, and use of information and other SA GAMING assets by third parties should be limited by the security principles of least privilege, separation of duties, and need to know.

Third parties should conduct themselves in a professional manner according to the appropriate roles and responsibilities of their contractual agreements, and in an ethical manner by abiding by, enforcing and ensuring compliance with this Policy and all related SA GAMING standards, NDAs, procedures and documentation.

6.6.6 Monitoring and Review of Third Party Services

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. The SA GAMING engagement sponsor is responsible for the information processed by a third party during an outsourcing arrangement.

6.6.7 Managing Changes to Third Party Service

Changes to third party agreements, including NDAs, must be managed and approved by the SA GAMING personnel with signing authority for the engagement. All contractual documents must be reviewed by SA GAMING Legal. If cardholder data is shared with service providers, then contractually they must adhere to the PCI DSS requirements.

6.6.8 System Planning and Acceptance

A formal review and approval process, approved by the Security Management group, must be established for the acceptance of new systems and applications, as well as changes to existing systems and applications before being purchased or put into a production environment. All new systems and/or enhancements to existing systems must have a risk

analysis and a vulnerability scan performed to identify areas of vulnerability, and to ensure those areas are properly addressed prior to production deployment. An independent evaluation should be considered when selecting new applications. Periodic reviews of the software and data content of critical systems should also be conducted.

6.6.9 Capacity Management

The use of resources including storage and processing, should be monitored, optimized and projections made of future capacity requirements to ensure the required performance.

6.6.10 Protection Against Malicious Code and Mobile Code

All SA GAMING internal and contract personnel must take precautions to ensure that malicious code is not introduced into the SA GAMING environment. Software that will damage or hinder the performance of any SA GAMING information assets must not be generated; copied, propagated or executed.

SA GAMING approved software must be used to detect and remove viruses and malicious software. Appropriate anti-virus software is mandatory for all computer operating systems. The software must be actively enabled at all times, except when required to perform other administrative functions. The software must be configured to scan all files types when they are accessed.

Security awareness training must educate the user community on the dangers that can be caused by viruses and the company expense of eradicating viruses. The training must include guidelines on running anti-virus software, updating software releases and new definition files, and actions to take when a virus is discovered or suspected.

6.6.11 Back-Up

Data archiving provides the means for recovering significant quantities of data lost or damaged during an incident, including failure of a disk drive and malicious activity resulting in destruction of information. Every User and server administrator is responsible for ensuring the frequent backup of files that are either irreplaceable, have a high replacement cost, or are considered critical to SA GAMING business and the system.

6.6.12 Network Security Management

The SA GAMING network infrastructure must be designed, implemented and operated in a manner that ensures adequate protection of information assets. Only authorized and

trained personnel can make changes or install network components on SA GAMING networks. Operational responsibility for SA GAMING's network infrastructure should be segregated from computer system administration. Changes to the existing architecture must be carefully planned, tested and implemented via change control processes to avoid any adverse security impacts. Significant network changes must be piloted prior to full deployment.

6.6.13 Removal and Seizure

The installation of any equipment not currently on the approved list of network devices for SA GAMING's infrastructure network is forbidden unless approved by SA GAMING's senior management, following a formal risk assessment of the equipment, prior to installation.

Any unapproved device connected to the SA GAMING network will be removed by the appropriate personnel. Further, any device connected to the SA GAMING network, whether SA GAMING provided or not, is subject to seizure pending completion of an investigation.

6.6.14 Media Handling

Media must be controlled and physically protected during its lifecycle of creation, storage, retention and destruction. Procedures must be developed to protect documents, computer media, and system documentation from damage, theft and unauthorized access.

Information handling standards and procedures should be developed to ensure appropriate handling of all information.

6.6.15 Exchange of Information

Confidential information of third parties must not be accepted and SA GAMING sensitive information may not be disclosed except pursuant to Non-disclosure Agreements (NDA) being executed. Each such agreement should describe the confidential information being received or disclosed with the specification and protection requirements of that information.

6.6.16 Physical Media in Transit

Physical transport of media offsite must be controlled against unauthorized access, misuse or corruption. Security methods commensurate with the identified information classifications must be used to protect SA GAMING's sensitive information electronically transmitted via public networks. Electronic transmission includes, but is not limited to, E-Mail, FTP, electronic FAX transmissions and any other Internet transmission.

6.6.17 Electronic Messaging

Electronic messaging (not e-mail) or instant messaging should not be allowed. If the need for such communication is necessary those needs must be approved on a case by case basis by senior management. Additionally, all instant messaging must be kept confidential by the appropriate encryption.

6.6.18 Electronic Commerce Services

Electronic commerce can involve the use of electronic data interchange, electronic mail and online transactions across public networks such as the Internet. A set of standards must be developed to address the various threats facing electronic commerce including fraud, contract dispute and disclosure or modification of information; accessing data remotely via modem, prohibition of storage of data onto local hard drives, floppy disks, or other external media, and prohibition of cut-and-paste and print functions during remote access.

6.6.19 Monitoring

Audit Controls must meet the following items:

- Provide sufficient information for an after-the-fact investigation of loss or impropriety
- Provide end-to-end accountability for all significant events
- Record who did what, and when it was done
- Protected from unauthorized access, modification or destruction
- Capable of recording:
 - Invalid authentication attempts
 - Valid logins by administrative, special privileged users
 - Unauthorized data or transaction access attempts
 - Creation, modification or deletion of system resources
 - Actions taken by administration or special privileged users
 - Other relevant security events, as necessary
- The audit controls must be of sufficient size and configuration to maintain records for the specified retention period for auditing and security logs
- Systems and applications should be able to report, in real time, significant security events that present an immediate threat. Such reports should be directed to a device designed to immediately alert system management
- Network devices such as, but not limited to, routers and switches must have logging enabled to ensure logs for end-to-end activity can be maintained.

A centralized audit system to support analysis of security relevant events must be used. The centralized audit system must be configured to issue a fault notification and an electronic mail message whenever the following events occur:

- Auditing is turned off
- An audit file overflows

Audit trails must be archived as part of the daily backup process. The audit system must be capable of storing at least 30-days of audit files.

6.6.20 Clock synchronization

Internal system clocks on servers, routers, switches, desktop and laptop devices must be synchronized regularly. System administrators are responsible for ensuring proper synchronization. Clock synchronization is essential for a meaningful incident investigation.

6.7 Access Control

6.7.1 User Access Control

All information resource users, including system administrators, must be uniquely identified on each system accessed. System access must be restricted to a need-to-know basis and requires prior authorization from the Information Owner. The identity of the user, administrator and any other person or machine that accesses SA GAMING's information assets must be validated by authentication.

A SA GAMING's unique user id is to be employed for systems access controls for all employees, contractors and authorized third parties requiring access to SA GAMING networks and systems.

All users must be authenticated using a password or other stronger authentication mechanism acceptable to information security. For sensitive systems, or where a login is being performed remotely, consideration must be given to the use of more rigorous authentication techniques.

The password management standard must be followed for any information resource using passwords for authentication.

6.7.2 Review of Access Rights

Information resource access must be removed on or before a users' last day of employment or contractual obligation to SA GAMING.

6.7.3 Unattended User Equipment

SA GAMING assets must be secured at all times when left unattended. This includes, but is not limited to, physically securing all mobile equipment when unattended. At no time should any asset of SA GAMING be left unattended in a public place without all information being removed from view, either by a password protected screen saver or a computer shutdown.

6.7.4 Clear Desk and Clear Screen Policy

Information assets must not be located or used in areas where an unauthorized person could view confidential, sensitive or privacy regulated information. When this is unavoidable, users must exercise caution to prevent unauthorized persons from viewing SA GAMING sensitive data.

6.7.5 Network Access Control

Access to internal and external networks should be controlled. User access to networks and network services will not compromise the security of the network services.

6.7.6 User Authentication of External Connections

Appropriate authentication methods should be used to control access by remote users.

6.7.7 Equipment Identification in Networks

Automatic terminal identification should be used to authenticate connections to specific locations and/or portable equipment. This should be used to authenticate a session that can only be initiated from a particular location or computer terminal. An identifier in or attached to the terminal can be used to indicate whether this particular terminal is permitted to initiate or receive specific transactions. It may be necessary to apply physical protection to the terminal.

6.7.8 Remote Diagnostic and Configuration of Protection

Physical and logical access to diagnostic and configuration ports will be controlled.

6.7.9 Segregation in Networks

Networks should be segregated into functional groups of services, users, and information systems.

The capability of users to connect to or between shared and segregated networks should be restricted, in line with the access control standards set forth by the Information Security Policy.

Networks should have routing controls to protect the corporate from network breaches or attacks. These will ensure that computer connections and information flows are not interrupted.

6.7.10 Application and Operating System Access Control

Security facilities should be used to restrict access to operating systems to authorized users. Access to applications and operating systems should be controlled by a secure log-on procedure. A suitable authentication technique should be chosen to substantiate the claimed identity of the user.

Sensitive applications and systems should be segregated from general access networks and additional controls should be placed on such systems and applications.

6.7.11 Mobile Computing and Teleworking

Each person performing work for, or on behalf of, SA GAMING must be diligent in his or her efforts to protect the corporate's information assets, especially when telecommuting or working from a remote location. Groups authorizing persons to telecommute or work remotely must provide the person with the resources necessary to protect SA GAMING's information assets.

Telecommuting requires employees to use either a SA GAMING provided secure remote laptop or PC to ensure the protection of SA GAMING's information assets as described in this standard.

Contractors are required to verify the use of an anti-virus software product with current downloaded signatures on their systems before accessing SA GAMING's network if a SA GAMING provided secure system is unavailable.

6.8 Information Systems Acquisition, Development and Maintenance

6.8.1 Correct Processing in Applications

The designated Information Owner of systems and applications must ensure procedures are in place for the operational monitoring of all production systems and applications. System requirements for time stamped logs and other security policies and standards for logging should be produced to aid in evaluating the operations.

The Information Owner is responsible for ensuring systems are in place to validate input and output data, as well as message integrity from associated systems.

6.8.2 Use of Encryption

Information that is determined to be sensitive will be protected using encryption as defined by SA GAMING Data Sensitivity Classification and Data Functionality Classification Standards. The cryptographic requirements will be followed as defined in the Encryption Use Standard.

Each individual user is personally responsible for all activities, whether intentional or unintentional, conducted under his/her userid(s), private signing keys, or other assigned resource(s).

All individual users should report any known or suspected security exposures, violations, or threats, whether accidental or intentional, to his/her manager and Security Management group.

If it is necessary to take encryption software to a foreign location, or to provide it to foreign nationals, the individual user is personally responsible to ensure full compliance with applicable law and regulations of the business unit's host country.

Non-repudiation services should be used where it might be necessary to resolve or protect against disputes about occurrence or non-occurrence of an event or action. It establishes evidence to substantiate whether a particular event or action has taken place.

6.8.3 Security of System Files

Access to system files and program source code should be controlled. IT projects and support activities should be conducted in a secure manner.

6.8.4 Security in Development and Support Processes

All developed, purchased systems or applications must contain the functionality to comply with SA GAMING's security policies and standards when developing, testing, and implementing new systems and applications. Each system/application must have at least one designated Information Owner who is responsible for all decisions impacting security and approving access to the application.

6.8.5 Change Control Procedures

Change Management procedures for requesting, authorizing, prioritizing, scheduling, distributing and communicating changes must be implemented for system and application maintenance or changes.

6.8.6 Restrictions on Changes to Software Packages

All changes to software packages must be approved by SA GAMING product support management in accordance with change management procedures for that business unit.

6.8.7 Outsourced Software Development

All outsourced software development must comply with SA GAMING information security policies, standards, and procedures. These development projects should be supervised and monitored by SA GAMING representatives.

6.8.8 Technical Vulnerability Management

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

Timely information about technical vulnerabilities of information systems being used should be obtained, SA GAMING's exposure to such vulnerabilities evaluated, and appropriate measures taken to address associated risks.

6.9 Information Security Incident Management

A breach of this policy may be considered a security incident. Due to the significant variance in severity of any set of incidents, procedures for response must be defined in a manner that first treat the incident as serious, and then proceed based on the actual severity of the incident as it is understood. Incident management plans must be

established to ensure a quick, effective and orderly response to all security incidents, including the following:

- Information system failures and loss of service
- Denial of service, intrusions or attempted intrusions
- Errors resulting from incomplete or inaccurate business data
- Viral contamination
- Breaches of confidentiality
- Security weaknesses in, or threats to systems or services
- Potential negative PR exposure

Incident reporting procedures must be addressed in New Hire Orientation and during the annual Security Awareness Training. The procedures must minimally address the following:

- The need for security awareness and to immediately report anything suspicious
- The procedure for an employee or contractor to report any suspicious activity
- An escalation procedure for reporting inside SA GAMING and identification of decision points for determining when to contact the Security Manager
- How to locate a list of contact information for all key individuals and groups
- Incident response procedures must be clearly defined, documented and tested at least annually

The incident response procedures must minimally address the following:

- The communication plan among the technology staff and decision makers within SA GAMING
- The procedure for beginning investigation of a reported incident
- The procedure for investigation recording and reporting
- The procedures for properly collecting and sufficiently protecting evidence for use in criminal or civil proceedings
- An escalation procedure for reporting to upper management, and identification of decision points for determining when to contact local law enforcement
- Designate specific personnel to be available on a 24/7 basis to respond to alerts
- Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems
- Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments

6.10 Business Continuity Management

SA GAMING Risk Management group must develop and maintain cost-effective business continuity plans that will ensure the continued operation of critical business functions and computer operations should a major business disruption occur. This plan should address the information security requirements needed for the organization's business continuity. Each business unit must designate an officer or group lead within the entity to be responsible for business continuity planning, testing and implementation when necessary.

6.10.1 Business Continuity and Risk assessment

Events that can cause interruptions to business processes should be identified. The business units should be responsible for maintaining a current Business Impact Assessment (BIA). Where appropriate, the business unit must implement and maintain a Disaster Recovery Plan for their location.

6.10.2 Testing, Maintaining and Re-assessing Business Continuity Plans

Business Continuity plans must be reviewed and tested on a regular basis that is acceptable to the Risk Management group and when major changes occur in the operating environment.

6.11 Compliance

SA GAMING must maintain compliance with all applicable national and international laws and regulations. Specific attention needs to be addressed to regulations and laws requiring compliance or certification to specific technical, procedural or other controls over personal or other protected information in transit or in storage.

6.11.1 Privacy of Personal Information

SA GAMING must maintain compliance with all applicable national and international privacy legislation in the relevant jurisdiction. SA GAMING has a responsibility to take reasonable measures to safeguard the privacy of all customers and employees, and to protect the confidentiality of all information under SA GAMING's control.

Each business unit must periodically assess the manner in which they come into possession of confidential personal information, and develop procedures to protect the same.

6.11.2 Copyrights

A copyright notice must be used to protect software or other copyrighted materials developed by or for SA GAMING. All copyrights of others must be honored and used in accordance with the copyright notice.

Information on the Internet may constitute published material protected by copyright law. Users are responsible for complying with copyright law and obtaining applicable licenses that may apply to software, files, graphics, documents, messages, and other material that are personally downloaded or copied by the user. Users may not agree to a license and may not download any material for which a registration fee is charged unless given prior written permission from their manager.

6.11.3 Licensed Materials

SA GAMING is bound by the licensing language for all software. All software is to be licensed to SA GAMING., not individual users.

Users of licensed materials, including PC software, must understand and adhere to the terms of the licensing agreement. Copies of licensed materials must be made only as specified by the license. Use of licensed materials is allowed only in accordance with the applicable licensing agreement.

6.11.4 Release of Corporate Information

Users must not forward or further distribute SA GAMING's sensitive information, inside or outside of the company, without authorization of the originator or appropriate manager. Management approval is required before anyone can post SA GAMING corporate information on public systems, bulletin boards or news groups. Any approved material that is posted must contain all proper copyright, trademark and disclaimer notices.

6.11.5 Records Management

Records and information are:

- SA GAMING assets that require economical and efficient management
- Created to conduct business

- Retained only as long as required by law or operational need

During the entire retention period, the recorded information must be organized in a logical, retrievable manner and stored under conditions appropriate for the length and type of use. SA GAMING business units are responsible for developing records management procedures for records generated or controlled by the unit. The records management procedures must apply systematic controls to managing records from creation through useful life to final disposal. Retention schedules for information, including backups, must be addressed in the procedures developed by each business unit.

7. Information Security Policy Exceptions

Any exceptions to this or any SA GAMING Information Security Policy, Standard, or Procedure must be applied for and authorization received in writing.