

GAMMIX STS B.V.

Information Security Policy

Summary

The objective of this Gammix STS security policy is to foster an environment that will secure information within the Gammix STS based remote gaming infrastructure from threats against privacy, productivity, reputation, or intellectual property rights.

The policy comprehensively applies to all individuals who interact in any way with the company's informational resources in any form.

It details each individual's responsibilities to prevent unauthorized access to physically available information (analog), and increasingly, electronic information (digital). It is designed to be consistent with THE REGULATOR policies and governmental laws that regulate specific types of information.

Version Management

Version	Primary Author(s)	Description of Version	Date Completed
1	IT Department	Draft of Policy	September 2023

Table of Contents

Summary	2
Version Management	2
Introduction	4
Purpose	4
Roles.....	4
Enforcement	4
Revision and changes.....	5
Structure of procedures within this policy	5
Organisation of information security	7
Asset management	7
Human resources security	8
Physical & environmental security	8
Communications & operations management	9
Access control	11
Information systems acquisition, development & maintenance	13
Information security incident management.....	15
Business continuity management.....	15
Compliance	16
Desktop and Laptop Computer Security.....	16
Media and Equipment Disposal	19
Data Classification.....	22

Introduction

The document describes types of transactions concerning betting accounts and security rules of player's money.

Policy

Purpose

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

This information security policy has been based on the international standards ISO/IEC 17799 (**Information technology - Security techniques - Code of practice for information security management**) and the Payment card Industry (PCI) Data Security Standard V1.2 (October 2008).

The objectives of this policy are:

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

Roles

- Information Security Officer (ISO)
 The ISO is responsible for ensuring that the Information Security Policy is implemented in Gammix STS business operations. The ISO is also responsible for all day to day information security issues and is the first point of contact for all security related issues within the organisation. The ISO liaises with the Key official on updates and implementations to the policies adhering to the regulatory authorities.
- Gammix STS Employees
- Third-party outsourced service partners

Enforcement

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

Revision and changes

All Gammix STS procedures are subject to an annual revision which has to be completed within October 31st. Significant changes to any policy or procedure has to be approved by the Key Official and communicated to the regulator.

Structure of procedures within this policy

Gammix STS policies and procedures are structured into categories. This document mentions most of the below procedures, in terms of information security and ISO 17799. Within the categories there are standalone documents which are focused on particularly critical or in-depth areas of Gammix STS business.

General procedures

Internal Audit Procedure + Checklist
Roles & Responsibilities
Business Continuity Plan
Risk Assessment Policy & Procedures

Operational procedures

Operational Checklists – Monthly & Yearly
Incident Response Procedure & Reports
Network Infrastructure & Remote Access Policy & Procedure
User Management Policy & Procedures
Access Control Policy & Procedure
Back-Up Policy & Procedure
Change Management Policy & Procedure
Data Classification & Protection Policy & Procedures
Office Environment Policy & Procedure
Player Monitoring Procedures, Reports & Logs

Financial procedures

Financial Checklist – Monthly
Financial Reporting to the regulator
Internal Financial Reporting
Approval Process for Financial Transactions
Financial Reporting & Reconciliation with APCO
Fraud Screening Procedure

HR procedures

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

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

1. Organisation of information security
2. Asset management
3. Human resources security
4. Physical & environmental security
5. Communications & operations management
6. Access control
7. Information systems acquisition, development & maintenance
8. Information security incident management
9. Business continuity management
10. Compliance

Organisation of information security

Policy objective

Provide guidelines for how the Information Security Officer (ISO) effectively should manage information security within the Gammix STS organisation Scope. The ISO may delegate some or all of the policy sections but is ultimately responsible for its implementation.

Procedure guidelines

- An Information Security Officer (ISO) and a deputy must be appointed to be responsible for all day-today security issues and be the central point of contact for security issues and incident management.
- The Group employs over 180 employees therefore security is key to our operation.
- The Gammix STS Management should meet at least once a year to review the current status of Gammix STS information security, approve new or modified security policies and other high-level security management activities.
- The ISO maintains a list of contacts in authorities such as law enforcement, money laundering and regulatory bodies, emergency services, health & safety and services providers (power, water, cooling etc.). The key official also assists the ISO in this area.
- The ISO should maintain contact with third party companies and confirm that special interest groups or other specialist security forums and professional associations assist in the protection of the gaming setup. Third parties are requested to abide by the Groups policies.
- The ISO must ensure that all contracts and agreements with 3rd parties comply with Gammix STS security policies and include appropriate Non-Disclosure Agreements (NDA's).
- A set of information security policies, of which this document is one, should be written, agreed and communicated to all employees and 3rd party organisations so that security requirements and obligations are well understood by all concerned.

Asset management

Policy objective

Ensure Gammix STS information systems and assets are tracked and maintained in accordance with their sensitivity and criticality. This is confirmed due to the third party servers (Microgaming) where Gammix STSs game servers is hosted is held in line with regulatory requirements.

Procedure guidelines

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

Human resources security

Policy objective

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

Procedure guidelines

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

Physical & environmental security

Policy objective

Prevent unauthorised physical access, damage and interference to Gammix STS's premises and information assets. All buildings and facilities rented or operated by Gammix STS.

Procedure guidelines

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

Communications & operations management

Policy objective

Ensure the correct and secure operation of all Gammix STS information processing facilities.

Procedure guidelines

- Operating procedures should be documented, maintained and made available to all users who need them.
- As far as practical, duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or accidental modification or misuse of Gammix STS's assets.
- All 3rd party service definitions and delivery levels (service level agreements or SLA's) should be included in the legal contracts and agreements and monitored for compliance.
- All information, particularly contact and payment details must be verified as correct from more than a single source at initial take-on and whenever subsequently changed.
- Production application resource usage should be monitored, tuned and projections made of future capacity requirements.

- Acceptance criteria for all systems should be established and suitable tests of the systems carried out during development.

Backup

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

Operational procedures

- System and application logging must be enabled and log files must be protected from deletion, modification or unauthorised access where possible. The production application should only have read / write access to the log files (no delete) and DBA's should only have read access (no write / delete).
- Log files must be periodically reviewed by the Operations team and any unusual activity alerted to the ISO.
- The production CRM database must be used to generate daily exception reports of unusual customer activity. These reports must be reviewed on a daily basis by management.
- The production application must implement controls to ensure that winning gaming accounts that do not have existing bank details at the time of the win are not successfully targeted by identity thieves.
- The principal of "least privilege" should be used for all privileged users (i.e. Administrator / Operator / DBA should only have sufficient privilege to perform their daily work).
- All privileged accounts must be identifiable and accountable to an individual.
- Full-privilege accounts should be created for controlled use (i.e. credentials stored in a safe). These accounts are for use in exceptional or unforeseen circumstances and their use must be authorised by the ISO.
- All software and hardware faults must be logged and reviewed on a regular basis by the Operations team
- All clocks in the production environment must be synchronised to an accurate time source to enable log file cross-referencing.
- Detailed production system documentation, such as designs, diagrams and specifications, must be marked and treated as "Gammix STS Proprietary" and protected against unauthorised access.

Access control

Policy objective

Control access to Gammix STS's information, systems and applications within the infrastructure.

Procedure guidelines

- There must be a formal employee / contractor ("User") registration and deregistration procedure in place or granting and revoking access to all information systems and services within Gammix STS.
- All users should be given a unique user identifier, preferably common across all systems if access to multiple systems is required.
- It must be possible to track the access rights and privileges granted to individual users. The ISO must periodically review these access rights and privileges using a formal process.
- Generic accounts must only be used when there is demonstrably no alternative, and all generic accounts used should be recorded by the ISO, together with a list of individuals who have access to the generic accounts.
- All user passwords must be changed periodically (every 60 days) and be composed by a minimum of 8 characters. It should contain a mix of capital and lower case letters and at least two characters must be numeric or a symbol/punctuation character. This policy must be enforced where possible at the Operating System level.
- All production database systems must be configured with strong access controls and there must not be any vendor-supplied defaults in the production environment.
- The production application must strongly authenticate to the production database in a way that cannot also be used for unauthorised interactive access.
- The production application authentication to the production application must not use the same credentials that are also used elsewhere (i.e. in any test or staging environment).

Access to the Gammix STS application will be from four categories of user:

- Players - to play
- Gammix STS Support - to manage the system and user accounts
- 3rd Party Support - to manage day-to-day support

It must be possible for each category of user to freeze or restrict account usage. Players must be able to freeze or restrict access to their own accounts and Gammix STS / Support must be able to freeze or restrict access to all accounts.

Information systems acquisition, development & maintenance

Policy objective

Ensure that security is an integral part of all information systems within the Gammix STS infrastructure.

Procedure guidelines

- Business requirements for new information systems or enhancements to existing systems must specify the requirements for security controls.
- Data and databases used in test or staging environments must be sanitised and not contain any sensitive or confidential information.
- The ISO must maintain an awareness of new security vulnerabilities as they are discovered and assess the impact on the production and office environments.
- The production and office environments should be regularly audited for compliance with security policy and also initially audited before go-live.
- The production and office environments should be regularly penetration tested by a 3rd party, on at least an annual basis and initially before go-live.

Production environment

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

Application design

- Application software must be robust, self-checking, and not vulnerable to invalid user input or the deliberate or accidental corruption of information.
- All production applications must protect the confidentiality and integrity of the data that they use or rely on.
- All production applications must follow the latest version of PCI guidelines for the development of secure web applications. The ISO deputy is responsible for ensuring that the latest PCI version is communicated and understood by all developers.

- The production application must not be vulnerable to a simple Denial of Service attack such as an automated "first page" player registration.
- The production application must generate a secure audit trail of all activity which is digitally signed by the application and can be shown to be unmodified in a Court of Law.
- The application software must validate all customer-requested data changes by sending an automated email to the customer. This email must be responded to by the customer before the requested change to customer data can be made.
- The application must be able to reliably determine the country of origin of a player during the sign-up operation.
- The application must take all possible steps to ensure that player sign-up is legal in the country of origin of the player.
- The application web site must comply with common content-rating guidelines so that it can be blocked, if required, by relevant authorities.
- The application must comply with all relevant data protection legislation, particularly with regard to personal data.

Source code

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

Information security incident management

Policy objective

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

Procedure guidelines

- A security incident handling procedure must be written and agreed with Operations staff. Roles and responsibilities must be clearly defined together with levels of action/response and escalation procedures.
- All Gammix STS employees, contractors and 3rd parties must be required to note and report any observed or suspected security weaknesses in systems or services.
- There must be a mechanism in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.
- We keep a separate folder with all internal Incidence reports. In most cases, incidents also have to be reported to the regulator. Official incidence report forms are available in the Gammix STS operational office and at the co-location site.

Business continuity management

Policy objective

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

Procedure guidelines

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

Compliance

Policy objective

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

Procedure guidelines

- Statutory, regulatory and contractual requirements must be explicitly defined, documented and kept up to date. Given the large cash flows inherent in a gaming, particular attention should be given to compliance with Money Laundering regulations.
- All intellectual property rights and licensing terms for the use of proprietary software products must be respected and enforced within Gammix STS and by all contractors and 3rd parties.
- Critical data must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.
- Data protection and privacy must be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses.
- Managers must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

Desktop and Laptop Computer Security

Overview

Description

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

Purpose/Rationale

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

Applicability

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

This policy includes all computers (e.g., desktops and laptops), stand alones as well as those connected to the Gammix STS Network.

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

Failure to Comply

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

Policy

- Gammix STS will ensure reasonable physical safeguards to maintain desktop and laptop computers and peripheral equipment in such a way to avoid inadvertent disclosure of Gammix STS information.
- Gammix STS shall be responsible for secure installations, configurations, distribution, management and removal from service, of Gammix STS desktop and laptop computers. Gammix STS must document if these responsibilities are assigned to another program area or office.
- Gammix STS may withdraw permission for any or all business or personal uses of its network or information systems at any time.

Securing Desktop and Laptop Computers

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

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

Physical Security Measures

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

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

Peripheral Equipment

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

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

Unauthorized Software

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

Viruses

- Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).
- Suspected viruses should be reported immediately to the Help Desk.
- Viruses shall not be deleted without expert assistance unless instructed by Gammix STS.

Monitoring of desktop and laptop computers.

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

Technical Security

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

- All Gammix STS desktop and laptop computers shall be configured according to the Gammix STS desktop and laptop configuration standards.
- User identification (name) and authentication (password) shall be required to access the operating system of all desktop and laptop computers whenever turned on or booted.
- Terminal sessions shall be configured to log a user off the system during extended periods of non-use. The period of non-use shall be for no more than 60 minutes.
- Local hard drives shall not be accessible when a desktop or laptop computer is booted from mobile media, e.g., a diskette or compact disk.
- All information stored in a shared directory on the Gammix STS Network shall be backed up daily by Gammix STS .
- Gammix STS standard virus detection software shall be installed on all desktop and laptop computers, mobile, and remote devices and shall be configured to check files when read and routinely scan the system for viruses.
- Desktop and laptop computers shall be configured to log all significant computer security relevant events. (e.g., password guessing, unauthorized access attempts or modifications to applications or systems software.)

Policy exceptions

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

Media and Equipment Disposal

Purpose

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

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

Scope

This policy applies to all Gammix STS employees who authorize the disposal, handle the media or devices intended for disposal, or who are directly responsible for the disposal of media and devices containing sensitive data or protected information. This policy covers all fixed and removable storage devices owned by Gammix STS . This includes, but is not limited

to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), and PDAs. Any storage devices currently available, or that become available in the future due to new technology, are also covered by this policy.

Responsibility and requirements

Disposal and sanitation methods

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

Office Responsibilities

- Each office will designate an individual(s) to be responsible for assuring that protected information, as well as the hardware or electronic media on which it is stored, is properly destroyed and cannot be re-created.
- Each office will designate an individual(s) to oversee the monitoring process.
- Each office will designate an individual(s) to document disposal information beginning with the point of designation for destruction to final disposal.
- The chain of custody of the data will be established and maintained in the disposal documentation and will clearly identify the asset or media to be disposed, as well as the individual(s) responsible for its disposal.
- Disposal information will be kept for a period to be specified by Gammix STS .
- Each office will submit a report to the ISO on a semi-annual basis.

Policy and Operating Procedure (OP) Updates

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

Enforcement Authority

- The Information Security Officer (ISO) is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of Gammix STS's information security program and IT policies.

Violations and Disciplinary Action(s)

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

Definitions

- Degauss – To demagnetize data from storage devices in order to destroy the media so it is no longer usable.
- Device – Including but not limited to personal computers, laptops, handheld units (PDA's).
- Disposal - The final disposition of electronic data, and/or the hardware on which electronic data is stored.
- Employee - Individuals employed on a temporary or permanent basis by Gammix STS ; as well as contractors, contractor's employees, volunteers, and individuals who are determined by Gammix STS to be subject to this policy. For the purpose of this policy, this also refers to anyone using a computer connected to the Gammix STS network.
- Media Controls - Formal, documented, policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.
- Sanitization - The process of rendering data harmless

Data Classification

Data Classification

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

Systems

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

Applications

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

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

Exceptions

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

1.1 DCL Definitions

DCL1—Public

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

Examples: Advertising, product and service information, published research, presentations or papers, job

postings, press releases, instructions, training manuals, the terms and conditions of the gaming platform, odds, news, banner.

DCL2--Sensitive

While some forms of sensitive data are available to the public, the distinction between public and sensitive data for the purpose of this DCS is in how the information is made available. Therefore, sensitive data must be protected by authentication or identity verification and includes information that would not be openly shared with the general public. Sensitive data is intended for use within the company or within a specific workgroup, by the owner (for example the user itself), department or group of individuals with a legitimate need-to-know. Unauthorized disclosure of this information could adversely impact the company, individuals or affiliates.

Examples: Game statistics, User Transactions Details, User Details and so forth.