INFORMATION SECURITY POLICY

1. INTRODUCTION

This document provides direction on principles, objectives, controls and overall governance of information security at Three6Five KZN (Pty) Ltd ("Three6Five") with Company Registration Number: 2013/086091/07.

2. APPLICABILITY

2.1. This policy applies to all employees, temporary workers, interns and other workers at Three6Five its agencies, brands, business units, shared service centres, and authorised third parties (freelancers, contractors, consultants, suppliers, etc.). These groups are collectively referred to as 'engaged parties' in this policy.

2.2. Three6Five and its agencies (including brands, business units and shared service centres) are collectively referred to as "business affiliates" in this policy.

3. INTRODUCTION

3.1. Information Security

3.1.1. Information security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction to provide information confidentiality, integrity and availability:

3.1.1.1. Confidentiality ensures that the necessary level of secrecy is enforced and unauthorised disclosure is prevented;

3.1.1.2. Integrity is upheld when the accuracy and reliability of information and information systems are provided, and unauthorised modification is prevented;

3.1.1.3. Availability refers to reliable and timely access to information and information systems by authorised individuals; and

3.1.1.4. Information systems refers to sets of information resources organised for information collection, processing, maintenance, use, sharing, dissemination or disposal.

3.1.2. The terms "security" and "data protection" refer to information security and "systems" as information systems, in all security policy documents. The terms 'information asset' and 'information system' are used interchangeably in this policy.

3.2. Information Security Management System

3.2.1. An information security management system is the organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources required to establish, implement, operate, monitor, review, maintain and improve information security, based on business risk.

3.3. Security Principles

3.3.1. Three6Five adopted the following principles to provide and promote security:

3.3.1.1. Respect for the legitimate rights and interests of others (ethical use of security);

3.3.1.2. Transparency in achieving security objectives;

3.3.1.3. Proportionality of security controls to assessed or perceived risks;

3.3.1.4. Accountability of information and information systems;

3.3.1.5. Partnership through excellence and business enablement;

3.3.1.6. Collaboration among business and external stakeholders; and

3.3.1.7. Awareness and promotion of Security Objectives.

3.3.2. Three6Five defined the following objectives to provide and promote security:

3.3.2.1. Protect the information necessary to run the business and meet our strategic and operational goals and objectives;

3.3.2.2. Protect the information our clients / customers entrust us with and meet their security requirements;

3.3.2.3. Comply with applicable laws, regulations and contractual requirements; and

3.3.2.4. Manage security risks to acceptable levels.

3.3.3. Three6Five meets the above objectives through a combination of administrative, technical and physical security controls, also called “technical and organisational measures”.

3.3.4. Security policy statements provide high-level direction on such controls, which are the minimum requirements engaged parties must meet.

3.4. Security Policies

3.4.1. The table below shows Three6Five information security policy set, collectively called “Security Policies” or “Security Policy” in this and other security documents.

Policy Name	Purpose
Information Security Policy	Provides direction on principles, objectives, controls and overall governance of information security
Access Control Policy	Provides direction on controlling access to Three6Five information and facilities
Network Security Policy	Provides direction on protecting and securing Three6Five network
Cloud Security Policy	Provides direction on securely hosting or using internal or external cloud solutions
Acceptable Use Policy	Provides direction on the acceptable use of information assets and encourages responsible behavior for safeguarding information
Mobile Device Policy	Provides direction on the secure usage of mobile devices and “Bring Your Own Device” arrangements
Incident Response Policy	Provides direction on how to handle a breach / compromise of sensitive information in accordance with international and local laws and regulations

4. POLICY STATEMENTS

4.1. Security Policy Management

4.1.1. A security steering committee consists of members from a broad range of business areas of Three6Five, who have the responsibility to review security policies and ensuring alignment with business goals.

4.1.2. The Chief Executive Officer (CEO) of Three6Five, alternatively the duly appointed Information Officer approves security policy documents.

4.1.3. Security policies must be reviewed at least annually or earlier if deemed necessary by business needs.

4.1.4. Exceptions to security policies must be considered for review and approval granted by the Information Officer/s.

4.1.5. Three6Five is responsible for disseminating security policies and manages the security awareness, training and education program related to its employees and affiliates.

4.1.6. Security policies will align to best industry requirements for information security controls, and any superseding requirements.

4.1.7. Three6Five, agencies, business units or account teams must determine if additional security policies are required, relevant to their work areas.

4.1.8. They must then implement and manage those policies at the agency, business unit or account level. Such policies must supplement security policies, which are the baseline. An example is a client mandated security policy. In case of a conflict, the policy providing greater security, applies.

4.2. Information Security Organisation

4.2.1. The Information Security Officer (IO), manages and maintains Three6Five's security program.

4.2.2. Security is the responsibility of everyone in Three6Five. The IO manages the information security program and employees are required to protect the assets assigned to them.

4.2.3. Wherever applicable, segregation of duties must be applied to prevent unintentional or deliberate misuse of Three6Five's assets. Information security must be considered in the project management lifecycle or client servicing environment.

4.2.4. The IO must maintain contact with specialist security forums to keep up-to-date on emerging and current security threats and countermeasures.

4.3. Engaged parties | Employee Security

4.3.1. Screening or background checks must be performed as part of the recruitment process, in accordance with local laws, regulations, contractual requirements, applicable state and business requirements, classification of information and perceived risks.

4.3.2. Employees must sign a confidentiality agreement as part of on-boarding.

4.3.3. Confidentiality agreements must define information security responsibilities and duties that survive after termination or change or termination of employment.

4.3.4. Employees must take security training at the time of hire and annually thereafter, or when required by client contractual obligations or other business needs.

4.3.5. Whenever possible, an exit interview must be conducted to cover the return of assets and reinforce the surviving obligations of the confidentiality agreement and applicable disciplinary code and procedures.

4.3.6. Human Resources (HR) shall determine the applicable disciplinary procedures to be instituted against Employees who commit a confirmed security breach.

4.4. Asset Management

4.4.1. Three6Five assets, also called information assets, must be appropriately protected. Examples of such assets are:

4.4.1.1. Documented business processes and activities (electronic or physical);

4.4.1.2. Electronic information (data, spreadsheets, presentations, documents, notes, email, social media, etc.);

4.4.1.3. Physical information (papers, signs, posters, etc.);

4.4.1.4. Hardware (servers, laptops, desktops, printers, photocopiers, routers, switches, firewalls, mobile phones, tablets, computing devices, etc.);

4.4.1.5. Software (databases, applications, utilities, productivity software, cloud services, etc.);

4.4.1.6. Network (communication links, wired network, wireless network, etc.);

4.4.1.7. Employees (contractors, interns, etc., as defined in this policy); and

4.4.1.8. Facilities (offices, datacentres, server rooms, wiring closets, storage facilities, studios, etc.)

4.4.2. An accurate and up-to-date inventory of critical assets must be maintained.

4.4.3. Critical assets are those, which if compromised or lost, could cause significant business disruption or revenue loss.

4.4.4. An asset owner must be designated for each inventoried critical asset, though assets remain Three6Five property.

4.4.5. Asset owners must ensure assets are:

4.4.5.1. Inventoried, appropriately classified and protected, have access restrictions, are periodically reviewed for access and classification; and

4.4.5.2. Properly handled during deletion or destruction.

4.4.6. Asset owners may delegate some responsibilities to an asset custodian responsible for day-to-day asset management and administration.

4.5. Information Classification

4.5.1. The following information classification categories are used within Three6Five:

Classification Categories	**Definition**
Public Information	Information in the public domain Non-sensitive. No anticipated disclosure harm. Includes but is not limited to: a. News articles, office addresses, etc.; b. Content shared with the industry (e.g., award nominations, industry working groups, etc.); c. Content shared on public platforms.

Restricted Information	<u>Sensitive</u> Unauthorised disclosure which may very likely cause commercial, legal or branding damage to Three6Five. Includes but is not limited to: a. Information for internal sharing, storage and collaboration such as company policies, project wins, agreements (clients, suppliers, freelancers, etc.), project plans, client deliverables, insurance policies, etc. b. Information for external sharing, storage and collaboration driven by business needs, e.g., business contacts' information, documents for collaboration with clients, suppliers, industry partners, etc.
	Three6Five or client non-nuclear personal information (also known as personally identifiable information, or PII) such as email IDs, addresses and telephone numbers.
Highly Restricted Information	<u>Highly sensitive</u> Unauthorised disclosure will cause serious commercial, legal or branding damage to Three6Five. This includes but is not limited to: a. Three6Five or client nuclear personal information (also known as personally identifiable information, or PII) such as credit card numbers, passport information, Identity Numbers, driving license numbers, insurance policy numbers, criminal activities / information or health information that could be linked to an individual. b. Three6Five intellectual property (IP) such as unpublished patents, unpublished copyrighted materials, trade secrets, pricing models, business plans, undeclared financial results, etc. c. Any other information deemed to be confidential, with perceived high disclosure risks such as payroll information, financial information, network architecture diagrams, performance reviews/succession planning or other confidential HR processes.

4.5.2. Asset owners must classify information according to its protection requirements as determined by legal obligations, asset value, criticality and sensitivity to unauthorised disclosure or modification.

4.5.3. Adequate protection must be applied to information relating to its classification. The Information Classification and Handling Guidelines provide guidance on how information at each classification level is labelled, handled and protected.

4.5.4. Information asset owners or custodians must develop procedures on how information is accessed, used and destroyed.

4.6. Removable Media Security

4.6.1. Removable media must only be used if there is a business requirement.

4.6.2. Examples of removable media are backup tapes, CD/DVD/optical/Blu-ray devices, portable USB storage devices, external hard disk drives and enclosures or any other devices used to copy or store systems data.

4.6.3. Removable media must be encrypted, dependent on business requirements, classification level and the extent to which encryption is supported by technology.

4.6.4. Removable media contents must be securely erased if no longer required or not in use.

4.6.5. Removable media must be physically destroyed if the contents cannot be securely erased or if the media is unusable or at end of life, as per the manufacturer's specifications.

4.7. Information Backup and Restore

4.7.1. Information and software needed to run the business must be backed-up regularly.

4.7.2. Acceptable backup options include copying information to magnetic media (backup tapes) or multi-site data replication.

4.7.3. Successful and unsuccessful backup activities must be logged and backup records must be maintained.

4.7.4. Backup procedures must be documented and reviewed at least annually and records of the review must be maintained. Unsuccessful backups must be investigated and remediated in a timely manner.

4.7.5. Encryption must be considered for backup data based on business needs.

4.7.6. If encryption is not possible, adequate compensating controls must be implemented.

4.7.7. The extent of the type of backup (full, differential or incremental) and frequency must be decided based on business and security requirements and documented in backup procedures.

4.7.8. Backup media retained offsite must be documented and catalogued with the following minimum information: backup date, type (daily, weekly, monthly, yearly), date sent offsite, expiration date, identifiers (serial number, barcode, etc.), backup system software version required to restore information, and hardware required to read the media.

4.7.9. Information must be restored from backups when needed to meet business requirements. Successful and unsuccessful restoration activities must be logged.

4.7.10. Restoration procedures must be documented and reviewed regularly, at least annually.

4.7.11. Restoration activities must be checked and tested regularly to ensure they are effective and can be completed within the time required by service level agreements (SLAs) and information disaster recovery plans. Records of such reviews must be maintained.

4.8. Backup Media Handling

4.8.1. Backup media must be stored securely offsite (away from the primary information source).

4.8.2. The offsite location must be a significant distance away, to avoid impact by outages or disasters at the primary site.

4.8.3. Transportation time from the backup site to the primary site must meet service level agreements (SLA) and information disaster recovery timelines.

4.8.4. An offsite location is either an authorised service provider in the business of backup media storage or another secure location in a Three6Five office.

4.8.5. Backup media requires pre-authorisation to be taken off premises. Records of such authorisations must be maintained. If a third party is used for transportation, the identity of the third-party person receiving the media must be verified before it's handed over.

4.8.6. Records of media taken offsite temporarily or for storage must be maintained and audited regularly.

4.8.7. Appropriate physical and environmental protection controls must be applied to backup media at the remote site and during transportation. Manufacturer recommendations for temperature and humidity levels in the storage environment must be considered. Backup media must be stored in fireproof cabinets at secure locations.

4.8.8. Offsite media storage facilities must be security audited regularly. Third-party contracts must address the third-party's responsibility for removable media security and their participation in security audits and remedial actions, if applicable.

4.8.9. Storage providers' backup media records must be regularly reconciled with Three6Five media records, to detect discrepancies that could affect information restoration from backups. Records of such reconciliation activities must be maintained. Backup media reuse and frequency must be defined and documented in backup procedures.

4.8.10. Unusable backup media, including media reaching end of life, must be fully destroyed under supervision. If a third-party service provider is used for destruction, they must provide written confirmation that the backup media was successfully destroyed. Logs of destroyed media must be maintained and reviewed regularly.

4.8.11. Backup media information must be retained in accordance with the Data Retention Policy. If notified of a "litigation hold" or "suspension notice", relevant information must be preserved until it is confirmed that the "hold" or "suspension" has come to an end.

4.9. Physical and Environmental Security

4.9.1. Physical and environmental security requirements must be considered during design, build outs or improvements of existing Three6Five facilities (owned or leased offices, datacentres, server rooms, wiring closets, buildings, storage, etc.) to protect against natural disasters, unauthorised access, malicious attacks and accidents.

4.9.2. Access to Three6Five facilities must be restricted to authorised engaged parties only.

4.9.3. Suitable physical security access control mechanisms such as access card readers, turnstiles, biometric access, manned premises, intrusion detection system, etc., must be deployed as appropriate.

4.9.4. Security barriers must be deployed at Three6Five facilities to protect the physical security perimeter consisting of walls, fences, doors, ceilings, floors, etc., to prevent unauthorised access, damage or interference.

4.9.5. Secure areas must be designated or built depending on business requirements, protection requirements of the information assets in those areas and perceived risks.

4.9.6. Procedures for working in secure areas must be developed and maintained, and must cover controls such as secure area access, closed-circuit television (CCTV) monitoring, restrictions on photographic equipment, etc.

4.9.7. Examples of secure areas include in-house or third-party datacentres, offshore development centres (ODCs) that are built specifically to meet client requirements, and in-house or offsite backup media storage facilities.

4.9.8. Visitors must be granted access to Three6Five facilities for business reasons only. Records of visitors to non-public areas (i.e. areas excluding the front desk, visitor rooms, stairs, conference rooms, etc.) must be maintained. As appropriate, visitors must be escorted within Three6Five facilities by a representative of Three6Five and display temporary identification, if issued during their visit.

4.9.9. Considering the nature of Three6Five's business, Three6Five's facilities may not have designated delivery or loading areas but if applicable, delivery and loading areas must be monitored for unauthorised access and incoming and outgoing materials are registered.

4.9.10. Safeguards must be applied and regularly tested to prevent or mitigate damage to Three6Five facilities from fire, flood, earthquake, lightning and other natural and manmade disasters.

4.9.11. Information processing facilities must be monitored for environmental conditions including temperature and humidity.

4.9.12. Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference or damage, wherever possible.

4.10. Datacentres and Server Rooms

4.10.1. Three6Five will manage all datacentres (DCs) {if applicable} and server rooms (SRs), including technology infrastructure assets, across Three6Five.

4.10.2. Accurate inventory of all DCs and SRs will be maintained by Three6Five.

4.10.3. Exceptions to Three6Five's managed DCs and SRs must be approved by the Information Officer.

4.10.4. Access to DCs and SRs must be authorised by the appointed Information Officer.

4.11. Equipment Security

4.11.1. Equipment must be protected to minimise potential risks such as theft, fire, explosives, smoke, water, dust, vibration, electrical supply interference, electromagnetic radiation, vandalism and unauthorised access.

4.11.2. Equipment must be protected from power failures and other disruptions caused by failures in electricity, telecommunications, water supply, gas, sewage, ventilation, air conditioning, etc.

4.11.3. Equipment supporting critical business processes must be maintained and tested regularly according to manufacturer recommended service intervals. Maintenance records must be maintained.

4.11.4. Equipment, except assigned portable/mobile devices such as laptops, mobile phones and tablets, must not be taken offsite without approval. Records of incoming and outgoing equipment must be maintained and reviewed periodically.

4.11.5. Appropriate protection must be applied to protect laptops, mobile phones, tablets, etc., while working remotely from home or other offsite locations.

4.12. Information Disposal

4.12.1. Information which is no longer needed must be securely wiped from information assets such as laptops, desktops, servers, printers, tablets, smartphones, backup tapes and other removable media, before being repurposed and in accordance with the Data Retention Policy.

4.12.2. When information cannot be securely wiped from an information asset, the asset must be physically destroyed.

4.12.3. Records of information disposal activities must be maintained.

4.12.4. If a third-party is involved in secure disposal, they must provide a certificate with the date, asset details and secure disposal method used.

4.12.5. Hardcopies of information must be shredded if no longer needed, unless preserved in accordance with the Data Retention Policy (e.g., litigation holds, suspension notice, etc.).

4.12.6. Third-party shredding services must be considered if shredding in-house is not possible.

4.13. Clear Desk and Clear Screen

4.13.1. Unattended desks and other work areas must be kept clear of Highly Restricted information. Use locked cabinets where applicable, to store hardcopies of Highly Restricted information.

4.13.2. A password-protected screensaver must be enabled by default on computer screens. Screens must be locked whenever a computer is left unattended, even if this is only for a short period. It must activate automatically after no more than 15 minutes of inactivity.

4.14. Operations Security

4.14.1. Documented procedures for operational activities must be developed, approved, maintained, regularly updated and made available to Employees who need them. Operating procedures must cover one or more of the following: instructions to process and handle information, workflows, backups, media handling, dependencies, exception handling, support and escalation contacts, recovery procedures for system failures, logging, monitoring procedures, etc.

4.14.2. Formal documented change management procedures must be developed and implemented for critical business processes, information facilities and critical systems. Change management procedures must consider identification and recording of significant changes, planning and testing of changes, assessment of potential impacts including security risk assessment, verification, and communication to stakeholders, fallback/backout arrangements and provision of emergency changes, needed to resolve a security incident.

4.14.3. Business-critical systems capacity must be monitored and remedial actions taken to ensure availability and to support business growth.

4.14.4. System owners or information custodians must develop a documented capacity management plan for business-critical systems.

4.14.5. Development, test and operational environments must be physically or logically separated to reduce the risks of unauthorised access or changes to the operational environment.

4.14.6. Appropriate technology must be implemented to prevent, detect and recover from malware.

4.14.7. As a minimum, workstations must be protected by an antivirus program with updated signatures, and if found, malware must be removed or quarantined.

4.14.8. Critical system activities must be logged and reviewed regularly. Logging facilities and logs must be protected against tampering and unauthorised access. Logs must be retained in accordance with the Data Retention Policy.

4.14.9. System administrator activities on critical infrastructure systems must be logged and logs protected and reviewed to identify any anomalies. System administrators must not have the rights to delete their activity logs of their activities.

4.14.10. Critical information systems clocks must be synchronised with an accurate and single time source.

4.14.11. Software installation on operational systems must be controlled and follow change management procedures. Where applicable, vendor-supplied system patches must be maintained at the level or version supported by the vendor.

4.14.12. Information relating to any technical vulnerabilities of information systems being used must be obtained in a timely manner. Exposure to vulnerabilities must be evaluated and measures must be taken to address associated risks.

4.14.13. To minimise business process disruptions, audit requirements and activities involving the verification of operational systems must be planned and agreed with stakeholders.

4.15. System Acquisition, Development and Maintenance

4.15.1. Software/application refers to all commercial off-the-shelf (COTS) software or bespoke software/applications that includes, but is not limited to, productivity tools, business application, operating systems, development toolkits, monitoring toolset, etc., (on premise or software as a service (SaaS) based) which can be provisioned/leveraged to perform business functions, activities and operations.

4.15.2. Three6Five IT, and Procurement teams must be consulted from the initiation phase of software procurement/development/outsourcing projects, as well as for the selection of third party consulting/development/outsourcing partners.

4.15.3. Three6Five IT must be engaged in all non-functional reviews to ensure compliance with Three6Five IT guiding principles and adherence to IT, Security and Data Privacy standards/guidelines, including alignment to existing Three6Five strategic technology investments and direction.

4.15.4. Three6Five IT must approve the use of software/application and explicit approval must be obtained by the IO and CEO, prior to provisioning/deployment and usage of the same.

4.15.5. All technology-related purchases such as hardware, software, cloud solutions, technology services, etc. require a purchase order (PO), must adhere to Three6Five approval process, and to be paid in the normal procurement process. Credit card purchases for technology which may conflict with Three6Five policy may not be allowed.

4.15.6. Security requirements must be identified and included in the specifications for new information systems or enhancements to existing information systems. Security functionality testing must be performed during development.

4.15.7. Information in application services passing over public networks must be protected. The protection level must match the classification level.

4.15.8. Information in application service transactions must be protected to prevent incomplete transmission, misrouting and, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

4.15.9. Change control procedures must be implemented to control changes within the development lifecycle for on premise and third-party solutions.

4.15.10. Modifications to software packages must be limited to necessary changes, and all changes must be strictly controlled.

4.15.11. When operating systems are changed, business critical applications must be reviewed and tested to prevent any adverse impact on operations or security.

4.15.12. A secure development environment must be established and protected. Test information must be protected by applying access control, monitoring, logging and secure disposal measures.

4.15.13. If system development work is outsourced, it must be monitored. The following contractual arrangements must apply for outsourced work: secure coding, design and testing practices, acceptance testing, escrow arrangements (if applicable), documentation, licensing arrangement, code ownership, rights to audit and compliance with applicable laws.

4.15.14. Acceptance criteria must be established for new information systems, upgrades and new versions.

4.15.15. Vendor-supplied software used in operational systems must be regularly patched and maintained at a version supported by the vendor. Exceptions must be formally approved by Three6Five IT assessing information security risks.

4.15.16. Software patches must be applied when they help remove or reduce security weaknesses and when feasible for the business. Vulnerabilities and vendor patch releases must be monitored, and critical patches must be deployed immediately.

4.16. Business Continuity Management

4.16.1. Three6Five Business Continuity Management (TCRBCM) program consists of:

4.16.1.1. Geography-specific, agency-specific or function-specific business continuity plans (BCPs) for dealing with longer-term outages and disasters at a geography, agency or function level;

4.16.1.2. Project- or operations-specific recovery plans, referred to as business continuity recovery plans (BCRPs) are for dealing with longer-term outages and disasters specific to a critical project, client work or business operations, as determined by business needs; and

4.16.1.3. Technology-specific disaster recovery plans (DRPs) are for business-critical IT services and applications to minimise the effects of a disaster or disruption.

4.16.2. BCPs, BCRPs and DRPs are collectively referred to as business continuity management plans (BCMPs), which allow Three6Five to:

4.16.2.1. Respond immediately to emergency situations;

4.16.2.2. Protect lives and ensure safety; and

4.16.2.3. Reduce business impact and resume critical business functions quickly after a disaster.

4.16.3. A business impact analysis (BIA) must be conducted in areas with business continuity requirements, to determine the maximum tolerable downtime, disruption for activities and other overarching contractual, legal and regulatory requirements. The BIA is the basis for BCMP development.

4.16.4. BCM roles and responsibilities must be defined and documented in BCMPs. engaged parties must be trained to understand and know how to exercise the BCMP.

4.16.5. BCMPs must be tested and updated regularly to ensure they are up-to-date and effective. The latest versions of BCMPs must be made available to Employees who require them.

4.16.6. Where applicable, BCMPs must capture information security continuity requirements to ensure the required level of information security during an adverse situation. Information security controls in the BCMP must be tested regularly for validity and effectiveness.

4.16.7. Appropriate redundancy must be built into business-critical systems, third-party cloud architectures, network and facilities to meet availability requirements. BCMPs must take into account these redundant components.

4.16.8. Contact must be maintained with specialist security forums and authorities such as law enforcement, fire departments, utility companies, telecommunication providers, internet service providers and supervisory and regulatory authorities.

4.17. Information Transfer

4.17.1. Information must only be transferred to external entities (third-parties, suppliers, auditors, clients, government authorities, industry regulators, law enforcement agencies, etc.) on a business-need basis. Information must only be transferred to authorised individuals at the receiving entity.

4.17.2. Non-public information must be transferred securely. Electronic information must be encrypted in transmission if required by its classification level.

4.17.3. The Three6Five IT must be consulted before transferring Highly Restricted information to an external entity.

4.17.4. Three6Five's IO must be consulted and approve any transfer of information to law enforcement agencies. As applicable, Three6Five's Data Disclosure and Individual Request Response policies must be followed.

4.17.5. Extranet connectivity requirements must be assessed for security risks by Three6Five IT before implementation.

4.17.6. Transport layer security (TLS) or virtual private network (VPN) must be implemented for secure information exchange with business partners based on business needs.

4.17.7. For secure information transfer, agreements with external entities must be signed, with the exception of law enforcement agencies. Agreements must address the receiving entities' responsibility to maintain confidentiality and protect information transferred to them from loss, unauthorised disclosure and modification.

4.17.8. Suppliers and service providers must sign an agreement to participate in Three6Five's security risk assessment program and provide evidence of security controls implemented in their organisation, to protect Three6Five's information transferred to them. The agreement must include the external entity's responsibility to show evidence of information destruction after the intended use of information transferred to them is over.

4.17.9. If courier arrangements are used to transfer information, the agreement must include details of authorised courier services and the mechanisms they use.

4.17.10. The agreement must include the external entity's responsibility to inform Three6Five of any compromise or breach of information transferred to them, within a reasonable timeframe.

4.18. Secure Development

4.18.1. Security must be considered and applied across all phases of the software development lifecycle, namely, requirements gathering, design, development, testing/validation and release/maintenance.

4.18.2. In the requirements gathering phase, product security requirements must be defined in terms of confidentiality, integrity and availability. Additional requirements to comply with security or privacy standards and compliance needs must also be identified.

4.18.3. In the design phase, security requirements defined in the requirements gathering phase must be mapped to the product's internal functioning. The following must be considered: techniques to reduce the amount of code available to untrusted users, entry points available to untrusted users, reduced privilege levels, minimal services and techniques to understand how a successful compromise could take place.

4.18.4. In the development phase, secure coding practices must be followed to reduce or eliminate security risks of vulnerable code. Industry recommended practices for secure development must be considered as appropriate.

4.18.5. Secure code reviews must be considered and performed as required. A secure development environment must be established and protected.

4.18.6. In the testing/validation phase, the product's security functionality must be tested to ensure requirements are met. Three6Five's IT must perform penetration tests or vulnerability assessments based on business requirements. Test environments must be secured and data used for testing, must be protected. Access to the code repository must be restricted to authorised employees/individuals only.

4.18.7. In the release/maintenance phase, newly identified security vulnerabilities must be addressed with code changes, retesting and following systems development life cycle (SDLC) security practices from earlier development phases.

4.18.8. Three6Five's IT must provide secure coding practices training to Three6Five's developer community. Engaged parties involved in software development must take secure coding practices training. Others such as architects, project managers and testers involved in development must consider taking the training, if this is required by their roles.

4.19. Encryption

4.19.1. Information must be encrypted based on business needs and industry best practices, client or other business partner(s) contracts that explicitly state encryption controls are to be applied, legal or regulatory requirements to apply encryption and the results of risk assessments or perceived risks.

4.19.2. Encryption must be used during information transmission, storage, transportation and transfer to removable media.

4.19.3. Three6Five IT and its IO must be notified of data decryption requests received from an external agency, organisation or individual, including any law enforcement agency or regulator.

4.19.4. Consider using mutual authentication (server to client and client to server) when using public networks such as the Internet to transmit Highly Restricted information.

4.20. Information Security Management System (ISMS)

4.20.1. Business needs (contractual, regulatory or legal requirements, risks, etc.) must determine the areas of the business included in the ISMS scope. If driven by business needs, an ISMS must be established, implemented, maintained and continually improved.

4.20.2. The ISMS scope must be defined and documented. As a minimum, it must cover business processes, people, information assets and the organisation at the business unit, agency, team, geography or process/operations, level.

4.20.3. Pertinent business leaders must oversee ISMS program governance and identify information security requirements to support the business, document information security objectives to meet those requirements, ensure budget is allocated and resources are made available for ISMS activities, and information security roles and responsibilities of Employees in the ISMS scope are documented and communicated.

4.20.4. Employees must receive security documentation and be trained on ISMS implementation, maintenance, continual improvement and auditing activities.

4.20.5. Employees must manage the documented information to support ISMS requirements in their work areas.

4.20.6. Information security risks must be assessed and addressed. Security risk assessments must be conducted regularly and risk treatment plans must be prepared and followed.

4.20.7. Procedures to support ISMS requirements must be implemented. Change control procedures must be implemented. Outsourced business processes must be controlled and monitored.

4.20.8. Internal and external information security audits must be conducted regularly within the ISMS scope. Management reviews must be conducted regularly.

4.20.9. Documented evidence of audits, metrics and management reviews must be retained.

4.20.10. Corrective actions must be taken for non-conformities to ISMS requirements. Root causes of non-conformities must be analysed and addressed to prevent recurrence or occurrence elsewhere.

4.20.11. Changes to the ISMS must be considered and implemented based on business requirements, security risk assessment results, non-conformities and security incidents.

4.20.12. ISMS performance and effectiveness must be measured and evaluated through performance metrics. Continual improvement initiatives must improve ISMS suitability, adequacy and effectiveness.

4.21. Security Risk Assessment and Treatment

4.21.1. Three6Five's IT and IO establishes the security risk management program based on business requirements. Three6Five's IT and IO must develop procedures for assessment and treatment of security risks.

4.21.2. Security risks must be assessed regularly. Security risk assessment (SRA) must involve identification, estimation and evaluation of security risks.

4.21.3. Three6Five's IT and IO must maintain a risk register to track identified risks.

4.21.4. Security risk treatment must involve implementation of one of the following management decisions:

4.21.4.1. Mitigate: Apply controls to reduce the risk to an acceptable level;

4.21.4.2. Manage (accept): Knowingly and objectively accept risk, provided it clearly satisfies risk acceptance criteria;

4.21.4.3. Transfer: Transfer associated risks to other parties, e.g., insurers or suppliers; and

4.21.4.4. Avoid: Avoid risk by ceasing activities that would cause risk to occur.

4.21.4.5. An owner must be identified for each risk captured in the risk register. Risk owners must ensure assessed risks are treated within agreed acceptable levels.

4.22. Security Compliance

4.22.1. Applicable security-related legislative, statutory, regulatory and contractual requirements must be identified, documented and complied with.

4.22.2. Software and fonts must be purchased and used as per authorised procedures.

4.22.3. Software and fonts must be used legally as per the licensing agreement terms and in compliance with applicable law. Intellectual Property (IP) rights must be protected.

4.22.4. Important records must be protected from loss, destruction and falsification in accordance with statutory, regulatory, contractual and business requirements and in compliance with the Data Retention Policy.

4.22.5. Personal data must be protected in compliance with laws, regulations, contractual requirements and business requirements, classification of information and perceived risks. The Data Privacy Policy provides direction on the use of personal data.

4.22.6. Encryption must be used in compliance with relevant agreements, legislation and regulations. Legal advice must be sought, as applicable, for hardware or software import or export for performing encryption or decryption functions, or to comply with government or regulatory orders.

4.22.7. Compliance with security policies and standards is mandatory. Corrective actions must be taken for non-compliance. Managers and supervisors are responsible for compliance in their areas of responsibility.

4.22.8. Information systems must be reviewed regularly for compliance with established security policies, standards and security best practices.

4.22.9. Independent reviews of the information security program must be considered and performed as determined by business requirements.

4.23. Supplier Security Management

4.23.1. The IO manages the supplier security risk management program to assess and address security risks associated with critical suppliers. Critical suppliers are those that have access to Three6Five's Highly Restricted information, e.g., cloud service providers, background check vendors, healthcare benefit providers, etc. Other suppliers, though important from a business perspective, are not as critical from a security perspective, unless determined by business needs, contractual requirements or perceived risks.

4.23.2. Critical suppliers must sign formal agreements with Three6Five before commencing services or gaining access to Three6Five's Highly Restricted information. Agreements with critical suppliers must include the following clauses: confidentiality, participation in Three6Five's supplier security risk management program, security requirements for protecting Highly Restricted information, notification to Three6Five of an information security breach / compromise and consequences following the breach, wherever applicable.

4.23.3. Where applicable, background checks must be performed for critical supplier personnel and security awareness or training materials must be provided to them for protecting Three6Five's information in their custody.

4.23.4. The IO must be consulted during the selection of critical suppliers, who are required to undergo a security risk assessment as per the protocols of the supplier security risk management program. If a security risk assessment is not possible at the selection stage, the IO must perform a risk assessment within 12 months of service commencement.

4.23.5. The IO must perform security risk assessments of critical suppliers.

4.23.6. The supplier point of contact (POC) must ensure assessed security risks are addressed by the supplier, as mutually discussed and agreed in consultation with the IO. The supplier POC must regularly update the IO on risk status until they are addressed by the supplier as recommended and agreed.

4.23.7. The IO must track supplier security risks until they are addressed to acceptable levels.

5. POLICY VIOLATION

5.1. Violation of this security policy is a security breach. Consequences of a confirmed breach may include disciplinary action up to and including termination of employment or contract, as well as civil or criminal action, or prosecution for each offense.

6. RESPONSIBILITIES

Stakeholders	Responsibilities
Three6Five Leadership	a. Provide direction and inputs for this policy and its enforcement. b. Support employees and initiatives involved in policy development, enforcement, monitoring and reviews.
Information Officer	a. Develop, enforce, monitor, review and update this policy annually or earlier as determined by business needs. b. Review the policy document classification level annually or earlier as determined by business needs. c. Review and approve waiver or exception requests with valid business reasons. d. Raise awareness and understanding of this policy across Three6Five via security education and awareness programs. e. Maintain the master copy of this policy document. f. Publish or distribute the full or redacted version of this policy document to the intended recipients.
Employees	a. Read, understand and adhere to this policy. b. Develop procedures to meet policy requirements. c. Consider policy statements as minimum requirements. Develop additional discretionary requirements, referencing this policy. d. Email the IO to report violations of this policy. e. Email the IO to submit feedback for improvement or ask questions related to this policy.