WOOLWORTHS FINANCIAL SERVICES

External Supplier Control Obligations
Information and Cyber Security

Version 8 May 2020

Control Area	Control Title	Control Description	Why this is important
Governance and Assurance	Roles and Responsibilities	The Supplier must define and communicate roles and responsibilities for Information and Cyber Security. These must be reviewed after any material change to the Supplier's operating model or business. Key roles must include a senior executive, accountable for Information Security.	Clear definition of roles and responsibilities supports the implementation of the Beam Schedule
	Governance	In order to protect WFS from Information and Cyber Risks, the Supplier must have risk governance processes in place that ensure an understanding of their technology environment and the state of security controls, and a security program to protect the Supplier from cyber threats in accordance with Good Industry Practice (e.g., NIST, SANS, ISO27001)	If this principle is not implemented, WFS or its Suppliers may not have and be able to demonstrate appropriate oversight on Information and Cyber security
	Strategy	Senior management approved policies, and standards to manage Supplier's Information and Cyber Risk must be in place and reviewed at least annually.	If this principle is not implemented, WFS data and critical infrastructure may not be protected by appropriate people, processes and technology leaving the bank open to significant risks from attacks.
	Information Security and Cyber Risk Reporting	Documented controls and processes must be in place to ensure Information and Cyber Security Incidents are reported and managed. Information and Cyber Security Incidents and breaches must be responded to by ensuring the appropriate processes and procedures are in place and reported to WFS immediately. An incident response process for timely handling and reporting of intrusions involving WFS' Information and/or Services used by WFS must be established. The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and shared and agreed with WFS.	An incident response process helps to ensure that incidents are quickly contained and prevented from escalating
	On-going Monitoring	The Supplier must regularly and in any event not less than once every calendar year, measure, review and documents its compliance with this schedule.	Ongoing monitoring is necessary to provide senior management with assurance over the design and operation of Information Security controls.
	Adherence to local legislative and statutory requirements	The Supplier must ensure that Information security related legislative and statutory requirements which apply to the jurisdiction in which the Supplier operates are complied with and that such compliance is appropriately documented.	Failure to comply with local legislative and statutory requirements could have serious repercussions for both the Supplier and WFS including fines, and in extreme case loss of WFS' banking license

Control Area	Control Title	Control Description	Why this is important
Education and Awareness	New Joiner education and awareness	The Supplier must ensure that all new Supplier Personnel, within a reasonable time period, complete training which ensures they understand their Information Security roles and responsibilities.	To ensure that all Supplier Personnel understand their responsibilities in relation to Information and Cyber Security principles.
	On-going education and awareness	The Supplier must ensure that once a year all Supplier Personnel complete mandatory training ensuring that they are aware of their Information Security roles and responsibilities.	
	Cyber Security Awareness	Enhanced cyber security awareness training must be delivered to system administrators at least annually to educate on scenarios/threats specific to their role, how to identify cyber threats, how to protect against cyber threats, and how to report concerns.	
Information and Cyber Security controls	Protection	In order to defend against motivated and adaptive threat actors, the Supplier must implement a defense in depth approach to ensure the bypassing of a single control does not result in the success of a threat actor. Defenses must be aligned to current threats.	If this principle is not implemented, WFS assets may not be appropriately protected against cyber-attacks.
	Vulnerability Management	The Supplier must ensure that management of vulnerabilities is covered as BAU within their operations including processes to detect and remediate vulnerabilities in all systems and to prevent new vulnerabilities being introduced during change processes and new system deployments. All material issues the Supplier has decided to risk accept must be communicated and agreed with WFS. Where the Supplier develops applications for use by WFS, or which are used to support the service to WFS, processes and controls must be in place to identify and remediate vulnerabilities in the code during the development process. IT Security patches and security vulnerability updates must be installed through an approved process in a timely manner to prevent any security breaches. Supplier Systems that for any reason cannot be updated must have measures to protect the vulnerable system. All changes must be undertaken in accordance with the Supplier's change management process.	If this principle is not implemented, attackers could exploit vulnerabilities within systems to carry out cyber-attacks against WFS and its Suppliers.

	Security Protection Technologies	Devices used to access the WFS network, or process WFS data, must be hardened to protect against attacks. This includes, but is not limited to, limiting attack surface through disabling of un- needed software/services/ports, ensuring all deployed versions are within public support periods, malware protection and host firewall capabilities are in place and appropriately configured, and controls in place to mitigate exploitation attempts.	If this principle is not implemented, WFS and Supplier network and endpoints may be vulnerable to cyber-attacks.
	Endpoint Security	Devices used to access the WFS network, or process WFS data, must be hardened to protect against attacks. This includes, but is not limited to, limiting attack surface through disabling of un- needed software/services/ports, ensuring all deployed versions are within public support periods, malware protection and host firewall capabilities are in place and appropriately configured, and controls in place to mitigate exploitation attempts.	If this principle is not implemented, WFS and Supplier network and endpoints may be vulnerable to cyber-attacks.
	Denial of Service Mitigation / Detection	Denial of Service mitigation capabilities must be applied to Internet facing services which have are required to support services provided to WFS The Supplier must ensure that security detection capabilities are in place, including the ability to detect denial of service attacks against internet facing systems needed to support services provided to WFS.	If this principle is not implemented, WFS and its Suppliers may be unable to prevent a denial of service attack from achieving its objective.
	Monitoring/Logging	Real-time monitoring of networks and endpoints for potential security events must be in place. Intrusion detection and prevention tools and systems must be deployed at all appropriate locations on the network and output monitored accordingly to detect cyber security breaches. Event data must be collected and correlated from applicable system sources and sensors and analyzed to identify and understand attacks/incidents. . Upon identification of any material incidents and/or breaches of security controls, the Supplier shall ensure that the Incident Management Process is followed All key systems, including key applications, must be set to log key events and system time across	If this principle is not implemented, Suppliers will be unable to detect and respond to security breaches or recover and learn from events that have occurred on their network by analyzing relevant logs.
	Malicious Code / Malware Protection	The Supplier must protect against transferring Malicious Code to WFS systems, WFS customers and other Third Parties in accordance with industry standard methods e.g., NIST, ISO27001.	If this principle is not implemented, the Supplier's network and systems may not be adequately protected against malware attacks, which could impact WFS assets.

	Unauthorized Device and Software Detection	The Supplier must ensure that they have the capability and processes to detect, contain/quarantine and respond to unauthorized devices, and software identified as malicious. The use of mobile computing must be always configured securely to prevent any cyber security events and misuse	If this principle is not implemented, Suppliers may be unable to detect, remove or disable unauthorized, malicious device or software, thereby exposing WFS assets to cyber-attacks.
	Technical Recovery	Processes must be in place, or external services retained, to perform the following actions after a security incident: • Identify, assess, and manage the safe mitigation of backdoors, implants, and changes introduced by threat actors. • Identify, assess, and manage the mitigation of vulnerabilities leveraged by the threat actor across the Group. Ensure recovery steps taken by business and technology teams do not compromise investigations, response activity, or on-going network security.	If this principle is not implemented, Suppliers may have inadequate processes and procedures in place to recovery from cyber incidents, thereby resulting in an aggravation of the impact of cyber incidents.
	Information Assets	The Supplier must have a designated contact to liaise with the WFS Information Asset Owner. An Inventory of all appropriate IT assets used to provide service to WFS must be in place and there must be at least one review annually to validate that the IT asset inventory is current, complete and accurate.	Ownership of information assets is fundamental for adequate protection on information assets.
	Information Classification	The Supplier must ensure that controls in place meet the confidentiality, integrity and availability requirements of the Information Asset based on its classification. The classification will be provided by WFS.	The classification determines the level of control required for the information asset
	Registration and Classification	The Supplier must apply the WFS Information Classification Scheme (Table 3 in the Appendix A) to all Information Assets held or processed on behalf of WFS, or an agreed alternative scheme.	A complete and accurate inventory of Information assets is essential for ensuring appropriate controls
	Labelling	Where applicable the Supplier must label Information Assets as appropriate* in accordance with the requirements of the WFS Information Classification Scheme (or the agreed alternative scheme). • *Appropriate refers to the benefit of labelling balanced against the associated cost. For example, it would be inappropriate to label a document if doing so would breach regulatory anti-tampering requirements. • If there is a requirement to use non-standard labels (i.e., any label not in line with the agreed Classification Scheme scheme), this must be agreed with WFS.	Labelling helps to inform Users of the control requirements for the asset
	Secure Storage	Controls must be in place to protect Information Assets wherever they are stored (this applies to Information stored as part of structured and unstructured methods). Information Assets such as Cryptographic keys or passwords, which are used to protect or access other Information Assets, must themselves be protected by encryption or equivalent controls.	Information assets are typically stored together and as such represent a concentration of risk and must be secured

Control Area	Control Title	Control Description	Why this is important
Information and Cyber Security controls	Back ups	Backs ups must be protected in line with the Confidentially, Integrity and Availability (CIA) rating of the Information Asset. The frequency and method of back-up must be agreed with the Information asset owner If media needs to be transferred physically either to facilitate a back-up or to store off-site following a back-up, controls must be in place to ensure the security of the transfer (e.g., encryption of media, secure transport containers). Information Assets that have been backed up must have defined controls to ensure access is only granted when needed.	Backups store copies of information assets and as such must be subject to the same controls
	Secure Retrievals	The supplier must only release an Information Asset to an individual approved by WFS. A documented/ recorded chain of custody must be in place and maintained throughout the retrieval process. If media needs to be transferred physically to facilitate retrieval, controls must be in place to ensure the security of the transfer. Physical security control requirements are defined in the Physical Security Supplier Requirements (BEAM).	An appropriate chain of custody ensures that Information assets are secured from loss
	Approved Usage	The Supplier must produce and publish Acceptable Use Requirements informing Supplier Personnel of their responsibilities. The requirements on access and use must as a minimum cover the acceptable use of the Internet, Social Media, corporate email, instant communication, IT equipment that is provided by Supplier, Bring your Own Device (BYOD) equipment that is used to access WFS' Information Assets and employee responsibilities when handling WFS' Information Assets. The Supplier must take appropriate steps to ensure compliance to the Acceptable Use Requirements.	Acceptable Use requirements helps to underpin the control environment protecting information assets

Information and Cyber Security controls	Logical Access Management (LAM)	LAM control objectives must apply to all types of IT System Accounts (User, Privileged User, Functional, and Shared). The Supplier must agree and document responsibilities for implementing the LAM control objectives shown within this Schedule, and for reporting their effectiveness. Individual accountability for each account must be in place (when shared accounts are used, accountability for them must be achieved through additional controls and processes as appropriate to the risk). The principles of least privilege and segregation of duties must be achieved for all accounts and account combinations. Authentication of an individual must take place before access is granted to an IT system. Authentication must be achieved securely and with complexity relevant to the risk of the accessed Information Asset (e.g., multi factor authentication, password complexity, encryption over authentication). Access management processes must be defined and include the following as minimum: • Account provisioning and authorizations must be in place to ensure that there is sufficient oversight over the creation of new accounts and the access levels provided • Processes for the change of access rights, revocation of access rights, suspension of access and removal of accounts along with defined time frames based on the risk levels of Information Assets accessed • Processes for a risk based periodic review and approval of access right Mover controls must ensure the Supplier requests /amends access relating to any Supplier Personnel moving roles within five (5) working days of the move date. Leaver controls must ensure requests to delete / disable access is executed by the account administration team according to the following schedule: • Network and Remote Access Account requests must be actioned within 24 hours • If the user gives notice in advance, the Line Manager must raise the appropriate deletion • request(s) on or before the user's last working day. • If the user does not give notice in advance (e.g., user sends resignation on or later than the last day in office), the Line Manager must raise the appropriate deletion request(s) within 24 hours of accepting the resignation i.e., contractual end date • If the user does not notify the organization, the Line Manager must raise the appropriate deletion request(s) within 24 hours of termination date i.e., contractual end date • If the user is terminated, the Line Manager must raise the appropriate deletion request(s) within 24 hours of termination i.e., contractual end date • However, the Line Manager does not need to raise deletion requests where this is already automated (e.g., through HR systems) For the sake of clarity, the Last Working Day, Last Day in Office and Contractual End Day shall mean the same. In situations where they happen to be different, due to certain business and geographical nuances, Contractual End Day, the day when the firm recognizes the exit of employee in its records, shall be reckoned. All other Account requests must be actioned within seven (7) days.	Appropriate LAM controls help to ensure that information assets are protected from inappropriate usage

		Dormant Account controls must ensure that Supplier Personnel Accounts that are not used for sixty (60) or more consecutive days must be automatically suspended, or equivalent compensating controls applied.	
Information and Cyber Security controls	Access Methods	Information Assets must only be accessible by methods that can uphold the security requirements of CIA. These access methods must be documented and periodically assessed to ensure they maintain their CIA capability. Passwords for interactive Accounts must be changed at least every 90 days and must be different from the previous twelve (12) passwords IT System Owners must ensure that active privileged default IT System Accounts have their passwords changed after each use, and every 90 days at a minimum. Account controls must ensure Interactive Accounts are disabled after a maximum of five (5) consecutive failed access attempts Remote Access controls must only be permitted via mechanisms agreed by WFS and Remote Access must use multifactor Authentication.	Access management controls helps ensure that only approved users can access the information assets

Control Area	Control Title	Control Description	Why this is important
Information and Cyber Security controls	Unstructured information	Unstructured Information Repository Controls must ensure all unstructured information repositories have been identified and access to any unstructured information repository containing WFS' information Assets (classified as Secret, Confidential or Internal Only) must be configured on a need-to-know, need-to-have basis.	The identification of the unstructured information is the fundamental step in applying the correct control levels
	Information Sanitization	The supplier must not use WFS' production data in test environments without the data being obfuscated unless controls equivalent to production system controls are in place. WFS' Production cryptographic keys must not be used in test environments and test keys must not be used in production environments.	Test environments are often not as secure as production environments and as such any information asset in a test environment is at greater risk
	Data Leakage Prevention	The Supplier must assess the risks to which WFS' Information Asset Types may be exposed. The risks considered must be informed, at a minimum, by the threats and leakage channels listed in Appendix A: WFS Risk Assessment Minimum Requirements, Tables 1 and 2.	Appropriate data leakage prevention controls are a vital element of information Security, helping ensure that WFS' Information assets are not lost
	Secure In transit	Controls must be in place to ensure that WFS' information Assets (classified as Secret, Confidential or Internal Only) in transit are protected based on their classification through the use of encryption or equivalent controls. When Information Assets in physical form are transferred, the control requirements in the Physical Security External Supplier Control Requirements (BEAM) apply.	In transit controls protect WFS' information from interception and disclosure.
	Recipient Identity	The supplier must only send WFS information to Individuals authorized by WFS	Recipient Identity controls ensure that WFS are aware of where its information is being sent
	Destruction/Deletion/Decommission of physical and logical Information	Where required by WFS, the supplier must destroy any Information Asset, in either electronic or physical form, so that it cannot be re-assembled in a meaningful way.	Secure destruction of Information assets helps to ensure that WFS' Information assets not disclosure through loss or malicious activity
Information and Cyber Security controls	Perimeter defense	The supplier must maintain an inventory of external network connections, Internet accessible hosts and data transfers used to transmit WFS' data back to WFS or any third parties (including without limitation any subcontractors [of the Supplier]. Data transfers should be classified based on the classification of the Information asset transferred, have clearly defined owners and the connection be verified as secure.	Appropriate protection for the perimeter helps to ensure that the network and WFS' information assets are appropriately protecting.

	Internal Network Security	The supplier must store WFS' Information assets on a segregated network from other clients	A segregated network helps to ensure that WFS' Information Assets are an adequately protected from unauthorized disclosure
	IT System Protection	The supplier must apply patches to its systems following a risk-based approach to determine applicability and timetable. Anti-malware solutions must be in place were supported at OS level (e.g., workstations and servers).	IT system security controls are vital for the protection of WFS' Information assets.
	Secure Build Standards	The supplier must define and implement Build standards for all configurable out of the box software used in bulk (e.g., Operating Systems, databases) and firmware of commonly used infrastructure (e.g., SAN or Network devices). Build standards must document the minimum security requirements to be applied to the different version of software. The builds standards must be reviewed annually and updated as required.	Standard Build controls help to protect information assets from unauthorized access
	Security change reconciliation and audit logging	Compliance with the build standards must be monitored and reported to the designated member of staff at the supplier. Non compliances to the build standard must be remediated. Security changes (e.g., security configuration changes, modification of account privileges) must always create a log that is stored in a tamperproof environment.	Compliance with standard builds and controls that ensure that changes are authorized helps to ensure that WFS' Information assets are protected
	Portable device security	Portable devices must be rendered unable to access WFS' Information Assets if control over the portable device is lost (e.g., because of theft or malware takeover) and Data Leakage Prevention (DLP) controls must remain effective if a portable device is not connected to a network.	The use of portable devices is becoming more prevalent and as such controls ensuring their security are becoming more important
Information and Cyber Security controls	Application protection	The supplier must ensure that Applications must be developed using secure code practices and must have adequate LAM structures based on the Information Assets accessible through them.	Controls protecting application development help ensure that applications are secured at deployment
	Network Access and Remote Access	The Supplier must ensure that access to the internal network must be monitored and only authorized devices must be allowed through appropriate network access controls. Where remote access to WFS' Information Assets is allowed, sufficient authentication and authorization of the end point must take place taking into account the identity of the user, the type of device and the security posture of the device (e.g., patch level, status of anti-malware, rooted or not rooted mobile device, etc.). All IT Systems supporting services provided to WFS must be protected from lateral movement of attackers on the network through logical separation of device management ports/interfaces from user traffic, and the enablement of all available exploit mitigation controls in the operating system and installed applications and agents.	Network access controls help ensure insecure devices are not connected the supplier's network, introducing new vulnerabilities

	Threat Simulation	The Supplier must engage an independent IT security assessment / Threat Simulation covering IT infrastructure and applications. This must be undertaken at least annually to identify vulnerabilities that could be exploited to breach the privacy of WFS Data through Cyber Attacks. The test must be undertaken by a recognized Security Assessment Vendor and all vulnerabilities must be prioritized and tracked to resolution. Any or all issues which are risk accepted must be communicated and agreed with WFS.	If this principle is not implemented, Suppliers may be unable to assess the cyber threats they face and the appropriateness and strength of their defenses.
	Encryption	The supplier must review and assess encryption technology and cryptographic algorithms it uses to ensure that it is still fit for purpose. The strength of the encryption deployed must be commensurate to risk appetite, as it may have an operational or performance impact.	Up to date and appropriate encryption protection and algorithms ensures the continued protection of WFS' Information assets
	Root Cause Analysis / Lessons Learned for Information and Cyber Security Events	The Supplier must have processes and procedures to undertake a root cause analysis of both internal (to the Supplier) and external events and apply the lessons learned from such analysis to strengthen its cyber risk management capabilities.	If this principle is not implemented, Suppliers would be unable to identify the root cause of cyber incidents and learn from same.
	Continuous Improvement	The Supplier must continually learn from events and apply their learning to improve of cyber risk defenses	If this principle is not implemented, Suppliers will be unable to utilize learnings from previous events to improve and strengthen their control environment.
	Right of Inspection	The Supplier shall allow WFS, upon WFS giving not less than 10 Business Days written notice, to conduct a security review of any site or technology used by the Supplier or its Sub-contractors to develop, test, enhance, maintain or operate the Supplier Systems used in the Services in order to review the Supplier's compliance with its obligations. The Supplier shall also allow WFS to carry out an inspection immediately after a Security Incident. Any non-compliance of controls identified by WFS during an inspection shall be risk assessed by WFS and WFS shall specify a remediation timeframe. The Supplier shall then complete any required remediation within that timeframe. The Supplier shall provide all assistance reasonably requested by WFS in relation to any inspection.	If this principle is not implemented, Suppliers will be unable to provide full assurance of compliance to these security obligations.

Definitions	
Disaster Recovery Environment	An environment, consisting of hardware and software that provides an alternative processing facility to the production environment in the event of a disaster
Functional	An account that is not assigned to a unique employee id, which an IT system uses to access the same or different IT systems.

Information Asset	An Information Asset is defined as any singular piece or grouping of Information that has a value for the organization
Information Asset Owner	The individual within WFS who is responsible for classifying an asset and ensuring that it is handled correctly
Information lifecycle	The Information Asset Lifecycle describes the various stages through which Information Assets pass during their existence and they are: Create and introduce, Store, Access and Use, Share, Archive and Dispose
Least Privilege	The minimum level of access/permissions which enables a user or account to perform their business role.
Platform	The hardware and software which must be present and functioning for an application program to run [perform] as intended. A platform includes but is not limited to the operating system or executive software, communication software, microprocessor, network, input/output hardware, any generic software libraries, database management, user interface software, and the like.
Privileged	A Privileged account is an account that provides an elevated level of control over a specific IT system. These accounts are typically used for system maintenance, security administration or configuration changes to an IT system.
Production environment	A Live environment, consisting of Hardware and software that is used to store and process Information by end users for business purposes. This includes the Disaster Recovery environment.
Shared	An account granted to more than one WFS employee, consultant, contractor or agency worker who has authorized access, but individual accounts are not an option provided due to the nature of the system accessed (e.g., an WFS social media account, a Virtual Data Room account, an App store account).
Structured Information	Information usually stored in databases accessible by application systems.
System	A system, in the context of this policy, is people, procedures, IT equipment and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.
Test environment	An environment, consisting of software and hardware where changes are tested prior to release into the production environment .
Unstructured Information	Information stored in office automation file types (e.g. Microsoft office files), scripts or images
User	An account appointed to a supplier employee, consultant, contractor, or agency worker who authorized access to an WFS owned system without elevated privileges.

Appendix A: WFS Risk Assessment Minimum Requirements and Information Schema and Handling. Table 1: Threats

Threat	Description
Unauthorized modification of information	Unauthorized use of a computer system to modify information. This could be through a compromised account or by an authorized individual deliberately or accidentally exceeding their authorization.

Unauthorized disclosure of information	Accidental or deliberate unauthorized disclosure of: • Business information (e.g., project names, customer names, medical records and credit card numbers) • User access credentials (e.g. unique identifiers and authenticators), which should remain confidential
Theft of or unauthorized use of or access to software	Theft of WFS' software, whether WFS' proprietary software or licensed by WFS from third parties (e.g., programs, computer code, source code, and methodologies).
Unauthorized access to, or theft of WFS Information Asset	Unauthorized access to, or theft of: • WFS business information (e.g., customer lists, product designs, trade secrets or intellectual property) • Personally identifiable information (credit card numbers, employment IDs or medical records)
Theft or loss of mobile devices or portable storage devices containing WFS Information Assets	Theft or loss of portable computer equipment (e.g., equipment used by individuals in remote environments), such as laptops, tablets, smartphones and portable storage devices.

Table 2: Minimum set of data (information) leakage channels which must be considered as part of the Supplier's Information Risk assessment:

Channel	Examples
Email	Corporate email, webmail, other email
Web	Internet (e.g., social networks, wikis, chat rooms)
Removable media	Approved/unapproved use, back-up tapes, USB devices including memory sticks, portable HDD. Also optical media, smartcards etc.
Physical	Corporate devices (laptops, phones, tablets etc.) Personal devices (laptops, phones, tablets etc.) Documents / paper sources (notepads, flipcharts etc.) Non-paper sources (encryption key cards, smart cards etc.) Physical files
Printing	All printing – home, remote
File transfer	Website Cloud services Peer-to-Peer / IM FTP / Secure FTP Fax EDI (Electronic Data Interchange)
People	Social engineering Coercion Bribery Human error
Voice	Dictaphones Conference calls Recordings and voicemail
Networks & connectivity	Unsecured / personal networks Wi-Fi Remote access
Image	Photographic capture Webcams Video / CCTV

Table 3: WFS Information Classification schema

Classification Level	Unrestricted (Level 1)	Internal Only (Level 2)	Confidential (Level 3)	Secret (Level 4)
Definition	The 'Unrestricted' classification applies to information which is already in the public domain, or information for which unauthorized public disclosure would have no significant negative impact or consequences for WFS, its customers or its business partners.	The 'Internal Only' classification applies to information related to WFS internal operations or communications which is of general relevance to all employees and appropriate for distribution throughout the organization. Such information would not typically have any significant negative impact if disclosed to unauthorized personnel but could provide knowledge of WFS' internal operations which may not be appropriate for non-Employee's members.	The 'Confidential' classification applies to information which is proprietary to the organization or related to a sensitive or specific business process and is not appropriate or necessary for viewing by all employees. Such information may have a negative impact if it were disclosed to unauthorized personnel both internally and externally. Personal and financial customer information is classified as 'Confidential' by default (although some less sensitive customer information or individual customer records may be classed as 'confidential' dependent on the requirements of the Information Owner or risk assessment - see the WFS Data Privacy Policy for further details).	The 'Secret' classification applies to information for which unauthorized disclosure (even within the organization) may cause serious financial or reputational damage, significant loss of competitive advantage, or lead to regulatory sanction or legal action.
Examples	• WFS marketing materials. • Job advertisements. • Public announcements. • Content of WFS publicly accessible web sites. • • Publications	• Organization policies. • Internal announcements. • Employee names and internal phone directories. • Job functions. • Employee handbook. • Newsletters. • • Internal Communications.	• New product plans. • Client contracts. • Organization charts. • Employee contact lists. • Audit reports. • Legal contracts. • P&L reporting. • Sensitive Customer / Client information including financial and personal. • Strategies • Vulnerability Assessments. • Performance Appraisals	• Profit forecasts or annual financial results (prior to public release). • Information on potential mergers or acquisitions. • Strategic planning information. • Performance and compensation information specific to individuals. • Sensitive customer/client information including financial and personal data. • Exco Minutes.
Hard Copy Information and Removable Media (Physical) Description: Includes all printed documents and data storage media used to store WFS' Information such as CDs, backup tapes and removable devices.				

Table 4: WFS Information Classification scheme handling requirements throughout the information asset lifecycle

Classification Level	Unrestricted (Level 1)	Internal Only (Level 2)	Confidential (Level 3)	Secret (Level 4)
Labelling	• Not required.	• Not Required.	• All hard copy information containing • 'Confidential' information must carry a prominently displayed classification label on the cover page, and a visible classification label on every page of the document (e.g. in the header or footer of the document.) • All removable storage media/devices containing 'Confidential' information must be labelled and marked accordingly, e.g., CDs must be marked with a permanent marker etc. All removable media must be labelled with the highest classification of any information residing on it.	• All hard copy information containing 'Secret' information must carry a prominently displayed classification label on the cover page, and a visible classification label on every page of the document (e.g., in the header or footer of the document.) • Wherever possible, removable media is not to be used to store or distribute 'Secret' information. If it must be used all removable storage media/devices containing 'Secret' information must be labelled and marked accordingly (as per 'Confidential' information) and additional controls must be in place (see handling, storage and distribution requirements).

Handling and Storage	• No restrictions.	• Secure workplace practices such as a clear desk policy, must be followed. Information must be stored out of sight when not in use and only provided to other WFS Employees unless authorised by the Information Owner.	• Physical documents and removable media must be stored securely, in accordance with the “need to know” principle, when not in use for long periods, for example, overnight. • Printed documentation must be retrieved from printer trays, fax machines or photocopiers. • • Only store ‘Confidential’ information on removable media for as long as it is explicitly required.	• Physical documents and removable media must be stored securely, in accordance with the “need to know” principle, when not in use. • Printed documentation must be retrieved immediately from printer trays or photocopiers. • ‘Secret’ information stored on removable media must be protected with appropriate additional technical controls (e.g. using WFS approved encryption mechanisms).
Retention	• No specific requirements (although Employees are encouraged to dispose of this information as soon as practical).	• No specific requirements (although Employees are encouraged to dispose of this information as soon as practical, and at least annually, except if directed otherwise by the Business Unit Retention Schedule or Information Owner).	• Retain in accordance with the documented region/Business Unit specific retention schedules.	• Retain in accordance with the documented region/Business Unit specific retention schedules. • • ‘Secret’ information is more likely to be subject to legal or regulatory requirements so retention requirements and processes must be reviewed regularly (at least annually) to ensure they are current.

Classification Level	Unrestricted (Level 1)	Internal Only (Level 2)	Confidential (Level 3)	Secret (Level 4)
Distribution	• No restrictions.	• No specific restrictions, although information should be review for appropriateness before distributing externally (if in doubt check with the Information Owner). • Must obtain approval from the Information Owner.	• No restrictions for internal mail. • For external mail (e.g., being sent by courier or local postal service), do not mark the classification on the envelope. • For fax, ensure the address is confirmed, accurately entered and confirm immediate receipt. Each page of the document must be clearly numbered, in a format that includes the total number of pages.	• Use care when sending 'Secret' documents internally or externally. Only send to authorized named individuals and address the information accordingly. Obtain approval from the Information Owner before sending documents and follow any additional distribution controls they specify. • For internal and external mail, mark the classification on an inner envelope. This inner envelope must then be placed in an unmarked outer envelope. • Use recorded delivery for 'Secret' Information delivered by external mail. • 'Secret' information must not be sent via fax.

Disposal	• No restrictions.	• Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder. • Delete information on removable media when no longer required.	• Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder. • Magnetic media (e.g., disks and tapes) that are no longer required must have the magnetic surface removed and cut into small pieces. • Optical media (e.g., CDs) must be scored with an abrasive material and, where practical, broken into pieces. • If re-usable media. Then all 'Confidential' data must be deleted /overwritten when no longer required and before re- use. • 'Confidential' data must be securely disposed of in accordance with supporting data disposal procedures	• Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder. • Magnetic media (e.g., disks and tapes) must have the magnetic surface removed and cut into small pieces • Optical media (e.g., CDs) must be scored with an abrasive material and, where practical, broken into pieces • If re-usable media. Then data must be securely overwritten when no longer required using an WFS approved secure deletion solution. • 'Secret' data must be securely disposed of in accordance with documented data disposal procedures, including recording the successful deletion of the information.