WOOLWORTHS FINANCIAL SERVICES

External Supplier Control Obligations
Records Management

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 Records Management. 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 Records Management.	Records Management requires high-level sponsorship to ensure that controls are designed, implemented, and operated effectively. Ongoing monitoring is necessary to provide senior management with assurance over the design and operation of Records Management controls.
	Records Management Risk Reporting	Documented controls and processes must be in place to ensure Records Management incidents are reported and managed. Records Management Incidents and breaches should be responded to by the Supplier 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 should 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.	
	On-going Monitoring	The Supplier must regularly and in any event not less than once in every calendar year, measure, review and document its compliance with this Schedule.	
	Adherence to local legislative and statutory requirements	The Supplier must ensure that Records Management related legislative and statutory requirements which apply to the jurisdiction in which the Supplier operates are appropriately documented and complied with.	

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, complete training which ensures they understand their Records Management roles and responsibilities.	To ensure that all Supplier Personnel understand their responsibilities in relation to Records Management If these requirements are not implemented then it may result in WFS' information not being retained in line with the applicable legal, regulatory, or business requirements, which may result in legal and regulatory sanction, reputational damage, loss / disruption of business.
	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 Records Management roles and responsibilities.	
Records Management Retention	Legal and regulatory retention requirements	The Supplier must ensure all Relevant Records are retained and disposed of in line with applicable legal, regulatory, or business requirements.	
	Retention schedule	The Supplier must ensure all Relevant Records are in line with the retention periods defined in the agreed WFS Retention Schedule. The Supplier must change the retention periods of Relevant Records, when instructed to do so by WFS.	
	Records Owner	The Supplier must nominate a key Supplier contact to be the liaison with the WFS Relevant Records Owner.	
Records Storage	Protection	The Supplier must ensure Relevant Records are protected using physical, environmental, and logical controls to prevent unauthorized loss, modification or damage throughout their retention and protected according to their confidentiality classification against the WFS Information Classification Scheme defined in the Information Security Supplier Control Requirements Schedule and the controls set out in the Physical Security Supplier Control Requirements Schedule.	If these requirements are not implemented then Relevant Records may be vulnerable to unauthorized modification, disclosure, access, damage, loss, or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business.
	Access	The Supplier must have physical / logical controls to ensure access to Relevant Records are restricted to only those Supplier Personnel who are appropriately authorized and need access to perform their duties.	
	Inventory	The Supplier must ensure an index / inventory of physical Relevant Records is maintained / be accessible to WFS and reviewed at least annually. The index / inventory must contain at least the following mandatory information: • Box owner • Box number • Description of contents • Destruction date or from date / to date	

Control Area	Control Title	Control Description	Why this is important
Records Retrieval	Retrieval	The Supplier must ensure Relevant Records can be retrieved within the following required timescales: • Electronic Relevant Records retrievable within three (3) working days or within a period required by any applicable legislative or statutory requirements; and • Physical Relevant Records / archived electronic records (not instantly accessible on a live system) retrievable within ten (10) working days, or within a period required by any applicable legislative or statutory requirements The Supplier must ensure retrieval processes are documented and the process tested at least annually through a testing regime or through business-as-usual processes.	If these requirements are not implemented then Relevant Records may be vulnerable to unauthorized modification, disclosure, access, damage, loss, or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business.
	Protection	The Supplier must protect Relevant Records during transit via appropriate controls (physical, environmental, logical) that are commensurate with the WFS Information Classification Scheme defined in the Information Security Supplier Control Requirements Schedule.	
Records Format	Authenticity and integrity	The Supplier must have controls in place to maintain and protect the authenticity and integrity of Relevant Records. The controls must be commensurate with the WFS Information Classification Scheme, set out in Appendix A - Table A and Table B. The Supplier must maintain records in a specific format required to comply with any applicable country legislation / regulation, such as maintaining relevant records in a non-rewritable, non- erasable format.	If these requirements are not implemented then Relevant Records may be vulnerable to unauthorised modification, disclosure, access, damage, loss, or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business.
Records Format	Scanned Documents	Where scanned documents are used as a Primary Record, the Supplier must ensure the Relevant Records are captured through a scanning process that: • Adheres to any applicable legal or regulatory requirements for the capture of scanned documents • Ensures quality assurance processes are in place commensurate to the value of the Relevant Records and classification requirements as listed in the WFS Information Classification Scheme; and • Captures scanned documents using a minimum of 200 dpi (dots per inch) scanning resolution/meet minimum industry scanning requirements.	

Control Area	Control Title	Control Description	Why this is important
Records Disposal	Disposal Process	The Supplier must ensure Relevant Records are securely destroyed within twelve months of the expiry of their retention period (upon notification and authorization from WFS), provided a Disposal Hold is not in effect.	If these requirements are not implemented then it may result in records being over- retained past their specified retention period or records being destroyed without authorization, which may result in legal and regulatory sanction, reputational damage, loss / disruption of business.
	Disposal Authorization	The Supplier must ensure evidence of the authorization and destruction of Relevant Records is maintained, using controls such as: • Physical Relevant Records certificates of destruction; and • Electronic Relevant Records audit trail / reports of Relevant Records purged / deleted For Suppliers of services to WFS, the Supplier must ensure WFS' Relevant Records are not destroyed without WFS' prior written consent. Service providers must confirm in writing the details of records that are destroyed. Evidence of the authorization and destruction of data and records must be maintained, using controls such as: • Physical certificates of destruction; and / or • Electronic records audit trail / reports of data and records deleted and / or • Destruction reports for storage media. (i.e., Hard Disks, cd's, microfiche);	
Records Disposal	Disposal Methods	The Supplier must ensure Relevant Records are disposed of safely and securely, through disposal controls which are: • applicable to legislative, statutory, and contractual requirements • commensurate with the Relevant Records confidentiality classification in the WFS Information Classification Scheme • applicable to the medium on which the Relevant Records are stored	
Records Disposal Hold	Disposal Hold Notification	The Supplier must have controls in place to ensure upon notification from WFS any Relevant Records covered by a Disposal Hold are suspended from destruction within 24 hours and confirm to WFS that the Disposal Hold requirements have been applied.	
	Disposal Hold Release	The Supplier must have controls in place to ensure upon notification from WFS of a Disposal Hold being lifted; any Relevant Records under the Disposal Hold have their applicable retention period or destruction recommenced within twelve months of the Disposal Hold being lifted (providing the records are not covered by another Disposal Hold).	

Records Management requirements	Original and Backup Relevant Records - Universal Time Coordinator (“UTC”) services	The Supplier must have controls in place to ensure an original and a backup copy of each electronic WFS Relevant Record are maintained and for all such electronic WFS Relevant Record(s) must implement and maintain Universal Time Coordinator (“UTC”) services, to ensure that file date/time stamp recordings and parameters are applied consistently.	If these principles are not implemented then it may lead to Relevant Records not being stored and retained in accordance with applicable regulations / legislation, which may result in legal and regulatory sanction, or reputational damage, loss / disruption of business.
	Relevant Records - Email	The Supplier must have controls in place to ensure emails generated by a Supplier and defined as WFS Relevant Records are retained for a minimum period of 7 years or specific retention period defined in the WFS Retention Schedule.	
	Letter of Undertaking	The Supplier must promptly provide the applicable regulator with a Letter of Undertaking if requested to do so.	

Definitions	
Disposal Hold	A notification to cease destruction of certain information, typically because the information may be required as evidence in a contractual, legal, or regulatory matter.
Letter of Undertaking	A letter from Supplier to a regulator of an WFS Entity stating that Supplier will take reasonable steps to fulfil any request by such regulator to download to any acceptable medium WFS Relevant Records that are maintained in electronic storage media within Supplier's possession or control.
Primary Record	Where duplicate copies of a Record exist, the Primary Record is the original version which is chosen to be used as the Relevant Record.
Relevant Records	Specific information required by WFS to be retained and disposed of in line with applicable legal, regulatory, or business requirements.
Relevant Records Owner	The owner of the WFS business process which the relevant records relate to may be the WFS Relevant Records Owner; or the Relevant Records Owner is assigned to the job role of the WFS person that created the Relevant Records.
Retention Schedule	A list of the Relevant Records which WFS are required to maintain and details the applicable country retention periods, any specific format / storage requirements, and the confidentiality classification of the Relevant Records.

APPENDIX A

Table A: 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 B: 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 authorized 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. • Maintain a record of data storage media containing 'Secret' information which is sent outside of the organization (e.g., to authorized Third Parties)
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.