WOOLWORTHS FINANCIAL SERVICES

External Supplier Control Obligations
Physical Security

Version 8 May 2020

Control Title	Control Description	WHY THIS IS IMPORTANT
1. Security Risk Assessments	Suppliers will ensure that annual security risk assessments are undertaken to review physical security measures and processes. Suppliers will ensure that identified gaps are addressed with a remediation plan (action, ownership, delivery date) and shared with WFS appropriately.	To ensure an accurate assessment of the Supplier's physical security environment, controls and processes and their current effectiveness. This may identify vulnerabilities and control gaps that have been inadequately addressed and reduce the risk of loss or damage of WFS' assets and associated reputational damage and/or regulatory fine or censure. They must be undertaken ahead of and/or in response to security activity as deemed necessary by the RSM/CSM. They must only be conducted by a member of the WFS team or a subject matter expert mandated by the RHS. Findings must be documented, action plans must be developed, and issues / risks identified must be escalated through the appropriate channels and thereafter tracked and monitored to closure.
2. Access Control	Suppliers will ensure that effective access control processes and systems are documented and deployed for all Supplier personnel. Access must be granted in line with the roles and responsibilities of the suppliers and must be controlled as per the zone table/restrictions in the AGPS Standard.	To ensure that only authorised personnel are permitted to enter areas of the Supplier's sites and thus reduce the risk of loss or damage to WFS' assets causing financial loss and associated reputational damage and/or regulatory fine or censure. In addition to the layered approach to security measures for premises where assets are normally situated or used, assets must be protected by security measures commensurate to their value and proportionate to the prevailing security threat in the location they are being stored and when they are being moved. Business must ensure that their business areas have procedures in place providing moveable assets with protection from theft or intentional damage commensurate with the value and risk. All employees must be provided with proportionate security advice, guidance and protection commensurate to their role and the threat environment. This applicable to any suppliers who are granted with access to WFS' buildings or assets.
3. Electronic Intruder Detection and CCTV	Suppliers will ensure that appropriate measures, including alarms, video motion detection and CCTV are deployed to monitor, detect and identify unauthorised access and security incidents. Equipment must conform to national and industry standards in terms of installation, operation, monitoring and maintenance. Images and data must be stored in secured, restricted areas, must searchable by date and time and must be retained for minimum period of 30 days, or in line with local laws and regulations.	To ensure that there is no unauthorised access to sites and buildings containing WFS' assets and data and that unauthorised access is detected in a timely manner.

4. Security Officers	Suppliers will ensure that security officers are deployed commensurate to identified risks requiring a physical presence to mitigate, or where electronic and/or remotely monitored systems would not provide effective mitigation. Security officers must be appropriately trained and deployed in line with local laws, regulations and licensing requirements.	If this requirement is not implemented, unauthorised access to sites and buildings containing WFS' assets and data may occur or may not be detected in a timely manner, increasing the risk of loss or damage to WFS' assets causing financial loss and associated reputational damage and/or regulatory fine or censure. In the event Security management has been outsourced, Suppliers will be responsible to follow all required protocols, these are specified in the AGPS Standard Some listed but not limited: a) All Tier 1 (e.g. critical injury / loss of life by employee / client / member of public) must be reported within 24 hours to the Chief Security Officer, WFS Key Risk Officer (KRO) and the RHS. All Tier 2 SSI must reported within 24 hours to the RHS and the Head of Security b) Tier 1 and 2's SSI must be reported and reviewed as part of the monthly Management Information (MI) and at the Security Forums. This ability will depend upon being able to identify, define and categorise types of incidents and having the necessary procedures, resources and competencies (including training and education) in place. c) All security incidents must be recorded on the authorised online security reporting tool i.e. CIES and must identify root cause, lessons learnt and any additional control requirements. d) The Head of Security is responsible for establishing procedures to investigate, grade, manage, document, escalate and respond to all security incidents. Procedures must be aligned to local incident management and business resilience structures. e) e. In order to provide an appropriate and flexible response to Security Incidents the Head of Security must have clearly defined procedures to ensure the implementation, monitoring and escalation of responses to incidents in line with prevailing Threat levels, whilst working collaboratively with other key

5. Security Incident Management and Response Levels	Suppliers will have in place procedures to manage security incidents and investigations. Where WFS' assets are impacted incident reports and investigation details shall be shared, including access control data and CCTV imaging where appropriate, and in line with local laws and regulations.	If this requirement is not implemented, WFS may not be able to gain confidence that Supplier has adequate documented and tested procedures to manage security incidents. This may lead to inappropriate action being taken following an incident, increasing the risk of loss or damage to WFS' assets or data and associated reputational damage and/or regulatory fine/censure. Security incidents must be effectively and consistently categorised, reported, escalated and managed using the ERMF matrix. A security incident is defined as a direct, indirect, or attempted act, which could result in the realisation of a Level 3 risk which includes harm to people (including employees or visitors); theft of, or intentional damage to, moveable assets; intentional damage to premises; and unauthorised access to premises. All Incidents must be managed in accordance with the framework provided by the Security Incident Management Plan (SIMP).
6. Transport	Suppliers will ensure that all WFS' assets and WFS' Data are transported securely.	To protect WFS' assets or data that may be transported between Supplier and/or WFS sites, decreasing the risk of loss, theft or damage and associated reputational damage and/or regulator fine/censure.