BARCLAYS

External Supplier Control Obligations

Physical Security (Technical Controls)

Version 13.0 September 2023

Control Title	Control Description	Why this is important
1. Access Control (TC 5.1)	Access control rules must be defined for all secure areas, supported with formal approved procedures, and defined responsibilities. Secure areas must be protected by appropriate entry controls and access points using electronic, mechanical, or digital access control. Logical and administrative access to electronic access control systems must be restricted to authorised personnel and access to physical keys and combinations must be strictly managed and controlled. An audit trail of credential/key/combination holders must be maintained, covering the granting, amending, and revoking of access permissions. All access credentials must be effectively managed to reduce the risk of unauthorised access. Access credentials must be managed in line with Supplier's access control procedures. Unique access credentials may be issued only upon receipt of the appropriate approval. All access credentials to restricted areas must be recertified at appropriate intervals. Where access to a premises or restricted area is no longer required, access credentials must be deactivated by the function responsible for the administration of access credentials within 24 hours of receiving notification from the relevant business unit or function advising of the change in requirements for the employee in question (e.g., change of role or responsibilities, or termination or employment).	Maintaining an effective access control system and access management processes and procedures is a vital component within the layered combination of controls required to protect premises from unauthorised access and to ensure the security of assets. Unless effective access control measures are in place, there is a risk that unauthorised personnel could enter Supplier's sites or restricted areas within its sites. This could increase the risk of loss or damage to Barclays' assets, causing financial loss and associated reputational damage and/or regulatory fine or censure.

2. Security of Perimeters, Buildings and Space (TC 5.2)	Security perimeters must be defined and implemented to protect areas that contain information and other associated assets, commensurate to the risk and threat environment identified and anticipated. Physical security for offices, rooms, and facilities (including access control systems, security cameras, intruder detection systems and other appropriate technical controls) must be designed and implemented on a risk-based approach based upon current and anticipated threat levels and be commensurate to the business processes undertaken and the information and asset value. Security processes for working in secure areas must be designed and implemented. Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities must be defined and appropriately enforced. All standalone, co-located and third-party data centres, cloud providers, data halls and communication installations (including server rooms and stand-alone communication cabinets) must be effectively secured to prevent unauthorised access and theft or damage to Barclays' assets or data. Where installations are in shared locations, effective security controls to effect discrete segregation and monitoring must be deployed	To protect Barclays assets or data held within data centres, data halls and supplier premises (both supplier-maintained and third-party) from the risk of loss, damage or theft resulting from unauthorised access to restricted space.
3. Protecting Against Physical Threats to Infrastructure and Assets (TC 5.3)	Protection against physical threats to infrastructure and assets must be designed and implemented through the deployment of security cameras, intruder detection systems and/or other layered security controls appropriate to the prevailing and anticipated threat environment. Premises must be continuously monitored for unauthorized physical access. Equipment must be sited securely and protected. Cables carrying power, data or supporting information services must be protected from physical interception, interference, or damage. Security equipment and installations must be	Deploying and operating physical security controls commensurate with current and anticipated threats will limit or prevent the impact of unauthorised access, theft or intentional damage to premises and assets.

	installed and maintained in accordance with the requirements of the manufacturer, and monitored to ensure availability, integrity, and confidentiality of information. Barclays assets held off-site must be protected at rest and in transit. Equipment must be installed and maintained correctly and to prevailing industry standards to ensure availability, integrity, and confidentiality of information. Installation and operation of all security systems must comply with prevailing Legal and Regulatory requirements. Where present, delivery and loading areas must be appropriately controlled and isolated from operational facilities to avoid unauthorised access and potential threat from unverified deliveries.	

This Standard must be read in conjunction with the following Standard, where the Management Controls identified as in scope must be applied:

Third Party Service Provider Control Obligation (TPSPCO), Management Control Requirements - Information, Cyber & Physical Security, Technology, Recovery Planning, Data Privacy, Data Management, PCI DSS and EUDA.