BARCLAYS

External Supplier Control Obligations

Physical Security (Technical Controls)

Version 12.0 October 2022

Control Title	Control Description	Why this is important
1. Access Control (TC 5.1)	Electronic, mechanical or digital access control must be deployed and managed in all premises undertaking activities relating to Barclays contracts. All security systems are to be installed, operated and maintained in accordance with legal and regulatory requirements. 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 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. Access credentials may be issued only upon receipt of the appropriate approval. All access 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). If remote working is required where Supplier or its subcontractors will access, store or process Barclays information in physical or virtual form that is restricted in nature (including personal data or any sensitive information which is provided to Supplier on a need to know basis),	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 their 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.

	Supplier must approve these arrangements with Barclays prior to allowing access to this data.	
2. Intruder Detection Systems and Security Cameras (TC 5.2)	Intruder detection systems (IDS) and security cameras must be deployed to deter, detect, monitor and identify inappropriate access or criminal activities. Equipment must be deployed proportionate to prevailing physical security threats identified by security risk assessments for each location. All camera systems and IDS must be installed, operated and maintained in accordance with current industry standards (for example International Organisation for Standardisation (ISO), System and Organisation Control (SOC), prevailing legal and regulatory requirements and current manufacturers specifications). Procedures must be in place to ensure IDS and security camera alarms are effectively monitored and managed. Access to the security system must be restricted to authorised personnel.	IDS and security camera systems are part of the layered controls to protect premises from unauthorised access and to ensure the security of assets. Unless these systems are effectively installed, operated, monitored and maintained, there is a risk of unauthorised access to sites and buildings containing Barclays assets and data, and that unauthorised access will not be detected in a timely manner.
3. Data Centres, Halls and Communications Installations (TC 5.3)	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. All data centres must have layered technical, physical and manned controls and site-specific procedures in place to effectively protect the perimeter, building and integrity of the data halls and all other critical areas. Controls include, but are not limited to, security cameras, intruder detection systems, access control and security officers. Where installations are	To protect Barclays assets or data held within data centres, data halls and similar critical locations from the risk of loss, damage or theft resulting from unauthorised access to restricted space.

	in shared locations, effective security around their discrete segregation must be deployed.	

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.