External Supplier Control Obligations

Physical Security

Version 10.0 Dated October 2020

Control Title	Control Description	Why this is important
1. Security Risk Assessments	Suppliers will ensure that Security Risk Assessments are undertaken to review physical security measures and processes. Assessments must be completed by a suitably experienced or qualified person, and must consider the appropriateness and effectiveness of physical security controls to mitigate both the current threat profile of the building and any emerging issues that may impact the site. The frequency of risk assessment activity should be in line with the purpose and criticality of the location. It is expected that sites critical to the operation of Barclays processes (including Data Centres) will be assessed at least annually. Security Risk Assessment findings must be documented, action plans must be developed and issues/risks identified must be assigned an owner and tracked through to conclusion. Barclays are to be informed of all significant findings within 10 working days of discovery.	Security Risk Assessments are a key requirement to provide an accurate assessment of the Supplier's physical security environment, controls and processes and their current effectiveness. They will identify new or existing vulnerabilities and control gaps and reduce the risk of loss or damage to Barclays assets and associated reputational damage and/or regulatory fine or censure.
2. Access Control	Electronic, mechanical or digital access control is to 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. Access to the system must be restricted to authorised personnel and access to keys and combinations is to be strictly managed and controlled. All access credentials are to be effectively managed to reduce the risk of unauthorised access. Access credentials are to be managed in line with the supplier's access control procedures. Access credentials are issued upon receipt of	Effective access control is part of the layered 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 the 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.

	the appropriate approval. All access to restricted areas is to be recertified at appropriate intervals. Where access to a premises or restricted area is no longer required access credentials are to be deactivated within 24 hours of notification.	
3. Intruder Detection Systems and Security Cameras	Intruder Detection Systems (IDS) and Security Cameras are to be deployed to deter, detect, monitor and identify inappropriate access or criminal activities. Equipment must be deployed proportionate to prevailing physical security threats identified during Security Risk Assessment activity for each location. All camera systems and IDS are to be installed, operated and maintained in accordance with accepted industry standards. Access to the 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 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.
4. Security Personnel	Security personnel are deployed proportionate to prevailing physical security threat at each location. All security personnel (whether employed by the supplier, a landlord or an external supplier) must be engaged or contracted through an accredited, licensed service provider in accordance with local legislation. Personnel must receive security training that is commensurate with their role and responsibilities. All training delivered must be documented and a training record must be maintained for all security personnel.	Security personnel are part of the layered controls to protect premises from unauthorised access and to ensure the security of assets. Unless Security Personnel are deployed in line with the prevailing security threat and appropriately trained, unauthorised access to sites containing Barclays assets and data may occur, or may not be detected in a timely manner. 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.
5. Security Incident Management and Response Levels	Suppliers will have in place procedures to manage security incidents and undertake investigations where appropriate. Where Barclays assets are impacted, the incident should be reported to Barclays with 48hrs and formal reports and investigation details shall be shared as soon as practicably possible, but no longer than 10 working days after the incident. This is to include access control data and security	If this requirement is not implemented, Barclays may not be able to gain confidence that the Supplier has appropriately documented procedures to manage security incidents. This may lead to inappropriate action being taken following an incident, increasing the risk of loss or damage to Barclays assets or data and associated reputational damage and/or regulatory fine/censure.

	camera imagery where appropriate, and in line with local laws and regulations.	
6. Transport	Suppliers will ensure that all Barclays' assets and Barclays Data are transported securely with proportionate controls in place commensurate to the value of the assets and data being moved (both from a financial and reputational damage perspective), and the threat environment in which they are being transported.	To protect Barclays assets or data in transit between the Supplier's and/or Barclays sites, decreasing the risk of loss, theft or damage and associated reputational damage and/or regulator fine/censure.
7. Data Centres and Halls	All standalone, co-located and third-party data centres, cloud providers and data halls are effectively secured to prevent unauthorised access and theft or damage to Barclays assets or data. All data centres are to 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. Controls include, but are not limited to, security cameras, intruder detection systems and access control.	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.