BARCLAYS

External Supplier Control Obligations

Physical Security

Version 9.0 Dated April 2019

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 Barclays 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 Barclays assets and associated reputational damage and/or regulatory fine or censure.
2. Access Control	Suppliers will ensure that effective access control processes and systems are documented and deployed for all Supplier personnel.	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 Barclays assets causing financial loss and associated reputational damage and/or regulatory fine or censure.
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 Barclays 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 Barclays assets and data may occur or may not be detected in a timely manner, increasing 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 investigations. Where Barclays 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, Barclays 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 Barclays assets or data and associated reputational damage and/or regulatory fine/censure.
6. Transport	Suppliers will ensure that all Barclays' assets and Barclays Data are transported securely.	To protect Barclays assets or data that may be transported between Supplier and/or Barclays sites, decreasing the risk of loss, theft or damage and associated reputational damage and/or regulator fine/censure.