BARCLAYS

External Supplier Control Requirements

Cyber Security

For Suppliers Categorised as High Cyber Risk

Version 6.0 Dated July 2015

Cyber Security Requirement	Description	Why this is important
1. Asset Protection and System Configuration	Barclays Data and the assets or systems storing or processing it must be protected against physical tampering, loss, damage or seizure and inappropriate configuration or changes.	If this principle is not implemented inappropriately protected Barclays Data could be compromised, which may result in legal and regulatory sanction, or reputational damage. Also services may be vulnerable to security issues which could compromise Barclays Data, cause loss of service or enable other malicious activity.
2. Change and Patch Management	Barclays Data and the systems storing or processing it, must be protected against inappropriate changes which could compromise availability or integrity.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.
3. Cloud / Internet Computing	Barclays Data stored in the cloud or on a public facing internet connection must be adequately protected via appropriate controls to prevent data leakage.	If this principle is not implemented inappropriately protected Barclays Data could be compromised, which may result in legal and regulatory sanction, or reputational damage.
4. Cyber Security Risk Management	Barclays Data and critical infrastructure must be adequately protected via appropriate people, processes and technology controls to prevent disruption of service or loss of data following cyber attacks.	If this principle is not implemented, then Barclays information may be disclosed and / or there may be loss of service leading to legal and regulatory sanction, or reputational damage.
5. Malware Protection	Anti-malware controls and tools must be in place to adequately protect against malicious software such as viruses and other forms of malware.	If this principle is not implemented, then Barclays information may be disclosed leading to legal and regulatory sanction, or reputational damage.
6. Network Security	All external and internal networks as part of the service must be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, external or internal networks could be subverted by attackers in order to gain access to the service or data within it.

Cyber Security Requirement	Description	Why this is important
7. Secure Development	Services and systems including mobile applications must be designed and developed to mitigate and protect against vulnerabilities and threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.
8. Security Assessment	Systems and services must be independently and rigorously tested for vulnerabilities.	If this principle is not implemented, then Barclays information may be disclosed and / or loss of service may occur leading to legal and regulatory sanction, or reputational damage.
9. Systems Monitoring	Monitoring and auditing and logging of systems must be in place to detect inappropriate or malicious activity.	If this principle is not implemented, suppliers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.
10. Bank Dedicated Space	For services provided which require formal Bank Dedicated Space (BDS), specific BDS physical and technical requirements must be in place. (Schedule 7 of contract the will confirm if BDS is a requirement for the service).	If this principle is not implemented, appropriate physical and technical controls may not be in place leading to service delays or disruption or Cyber Security Breaches occurring.
11. Cryptography	Confidential and Barclays Data must be encrypted.	If this principle is not implemented, appropriate physical and technical controls may not be in place leading to service delays or disruption or Cyber Security Breaches occurring.

1. Asset Protection – Minimum Control Requirements

Control Area	Control Title	Control Description
IT Asset Management	Inventory	An Inventory of all appropriate IT assets must be in place and there must be at least one test annually to validate that the IT asset inventory is current, complete and accurate
IT Asset Management	Physical Protection In Transit	All IT hardware must be physically protected during transit at all times
IT Asset Management	Backup media	All backup and archival media containing Barclays information used to provide the Services, must be encrypted and contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by the Supplier and in line with the Information Classification and Handling Schedule.
IT Asset Management	Secure Data / Media Disposal	Barclays Data / Confidential Information that is printed/written on paper must be destroyed securely as soon as it is no longer required. Data that is on media that is no longer required must be securely wiped so that information cannot be retrieved
IT Asset Management	Mobile Computing	The use of mobile computing must be configured securely at all times as per business usage of mobile devices policies and procedures to prevent Data Leakage and misuse

2. Change and Patch Management – Minimum Control Requirements

Control Area	Control Title	Control Description
Change and Patch Management	Change Management	All key IT changes prior to implementation must be logged, tested and approved via an approved , robust change management process to prevent any service disruption or security breaches
Change and Patch Management	Emergency Fixes	The Supplier shall ensure that Emergency Fixes are implemented when available and approved, unless this introduces higher business risks. Supplier Systems that for any reason cannot be updated shall have security measures installed to fully protect the vulnerable system. All changes must be undertaken in accordance with the Supplier's change management process.
Change and Patch Management	Patch Management	• The Supplier shall develop and implement a patch management strategy that is supported by management controls and supported by patch management procedures and operational documentation. The Supplier shall develop and implement a patch management strategy that is supported by management controls and supported by patch management procedures and operational documentation. • As soon as they become available, IT Security patches and security vulnerability updates must be installed through an approved process in a timely manner to prevent any security breaches. Supplier Systems that for any reason cannot be updated must have security measures installed to protect the vulnerable system. All changes must be undertaken in accordance with the approved change management process. • Open source applications are checked for outstanding vulnerabilities.

3. Cloud and Internet Computing – Minimum Control Requirements

Control Area	Control Title	Control Description
Cloud Computing	Cloud Computing	All use of cloud computing used as part of the service to Barclays must be approved by Barclays and controls to protect data and the service must be commensurate with the risk profile to prevent data leakage and cyber breaches.
Cloud Computing	Cloud Computing	• Assets must be located inside approved countries / locations including the disaster recovery locations. • Asset information much be captured including the virtual systems used to provide cloud services. Assets must be protected with DLP requirements, Anti-Virus, HIDS, NIDS, HD encryption, Cryptographic controls. A prior formal agreement for data transfer into cloud environments, portable storage, etc. must be in place for all the data classified and data inventories. • Backup media – must be encrypted. The encryption keys need to be secured and access restricted • All controls related to cloud services must be discussed and agreed with Barclays.

4. Cyber Security Risk Management – Minimum Control Requirements

Control Area	Control Title	Control Description
Cyber Security Risk Management	Cyber Risk Assessment	The cyber security risk profile to the organizational operations, assets, and individuals must be understood by • Assessing asset vulnerabilities • Identifying both internal and external threats • Assessing potential business impacts Risks and threats must be identified, prioritised and action taken accordingly to mitigate. The Supplier shall undertake regular Risk Assessments in relation to information security (and in any event not less than once every 12 months) and shall implement such controls and take such steps as are required to mitigate the risks identified. If a material risk identified that could adversely affect the reputation or service provided to Barclays, the supplier must notify Barclays within 24 hours.
Cyber Security Risk Management	Cyber Security Governance	Appropriate cyber security governance must be in place by ensuring that: • A specialist Information / cyber security function which has responsibility for integrating information security consistently into the Supplier's business is in place • The policies, procedures, and processes to manage and monitor the supplier's regulatory, legal, cyber risk, environmental, and operational requirements are understood, documented and in place and approved by Senior Management on an annual basis • The Supplier shall ensure that the information security status of critical IT environments (including the Supplier Systems), applications, computer installations, networks and systems development activity supporting the Services shall be subject to thorough and regular security audits/reviews conducted by an independent function within the Supplier's organisation. If a material vulnerability is identified that could adversely affect the reputation or service provided to Barclays, the supplier must notify Barclays within 24 hours.
Cyber Security Risk Management	Roles and responsibilities	• The Supplier must regularly and in any event not less than once in every calendar year during the term, measure, review and document its compliance with this Schedule. As a minimum, the Supplier must promptly and accurately complete the questionnaire provided by Barclays and return it within 20 business days. • Without prejudice to Barclays other rights and remedies, Barclays may risk assess any non-compliance reported by the Supplier to Barclays and may provide a timeframe within which the Supplier shall complete any reasonably required remediation.

Cyber Security Risk Management	Incident Response	Security incidents and data breaches must be responded to and reported to Barclays immediately and also progress on remedial actions. An incident response process for timely handling and reporting of intrusions involving Barclay's data and/or services used by Barclays must be established. This must also include an appropriate approach to forensic investigations
Cyber Security Risk Management	Awareness Training	Appropriate training material including cyber security awareness and ensures that all relevant employees are suitably trained to carry out their roles and responsibilities

5. Malware Protection – Minimum Control Requirements

Control Area	Control Title	Control Description
Malware Protection	Malware Protection	The most up to date Malware protection must be applied to all IT Assets used to provide the service at all times to prevent service disruption or security breaches • The Supplier shall establish and maintain up-to-date protection against Malicious Code / Malware in accordance with Good Industry Practice. • The Supplier shall protect against transferring Malicious Code to Barclays systems, Barclays customers and other Third Parties using Barclays Systems or Supplier Systems using current industry standard methods.

6. Network Security – Minimum Control Requirements

Control Area	Control Title	Control Description
Network Security	External connections	• The Supplier shall ensure that its network shall be designed and implemented so as to be able to cope with current and predicted levels of traffic and shall be protected using all available in-built security controls. • The Supplier shall ensure that its network related to the provision of the Service shall be supported by accurate, up-to-date diagrams that include all system components and interfaces to other systems, and be supported by documented control requirements and procedures. • All external connections to the network must be documented, routed through a firewall and verified and approved prior to the connections being established to prevent data security breaches
Network Security	Wireless access	All wireless access to the network must be subject to authorisation, authentication, segregation and encryption protocols ex. WPA2 to prevent security breaches. Any Wireless connection shall only be permitted from supplier locations must be approved by the Barclays
Network Security	Firewalls	• The Supplier shall ensure that all networks not owned or managed by the Supplier are routed through a firewall, prior to being allowed access to the Supplier's network. • Firewalls must ensure secure connections between internal and external systems and shall be configured as so to only allow the required traffic to pass through. Firewall configurations must be regularly reviewed to remove redundant or inappropriate rules and applicable sign off available to evidence.
Network Security	Intrusion detection / prevention	Intrusion detection and prevention tools and systems must be deployed at all appropriate locations on the network and output monitored accordingly to detect for cyber security breaches including Advanced Persistent Threats (APTs).
Network Security	Distributed Denial of Service (DDoS)	A defense in depth approach must be implemented in the network and key systems to protect at all times against service interruption via cyber attacks. This includes Denial of Service (DoS) and Distributed Denial of Services (DDoS) attacks.

7. Secure Development – Minimum Control Requirements

Control Area	Control Title	Control Description
Secure Development	Secure development methodology	All development must be undertaken in line with an approved documented Systems Development Methodology at all times. Secure coding standards must be in place and adopted in line with Good Industry Practice to prevent security vulnerabilities and service interruptions. The code to defend against possible well known vulnerabilities.
Secure Development	Environment segregation	All systems development/build must be undertaken in a non-production environment and segregation of duty enforced at all times to prevent data leakage and accidental data modification/deletion. There must be no live data in test unless agreed in advance by Barclays.
Secure Development	Live Data in Non-Production Environments	The Supplier shall ensure that live data (including Personal Data) will not be used within non-production environments without Barclays' prior written approval and agreement of the controls to be implemented to protect that live data. Where live data is used in non-production environments then the Supplier shall ensure that it must be secured to the same extent as the production environment after the approval from Barclays Data owner.
Secure Development	Secure Coding Practices	The Supplier shall have secure development practices for itself and any Sub-contractors, including the definition and testing of security requirements. Such practices shall be fully documented.
Secure Development	Segregation of Duties	The supplier shall ensure that segregation of duties is in place for system development, including ensuring that system developers do not have access to the live environment, unless in an emergency where such access would be protected with adequate controls such as break-glass procedures. Such activities in these circumstances shall be logged and subject to independent review.
Secure Development	Quality assurance	The quality assurance function must check that all the key security activities have been incorporated into the system development process to prevent service interruptions and security vulnerabilities

8. Security Assessment – Minimum Control Requirements

Control Area	Control Title	Control Description
Security Assessment	Penetration test	• The Supplier shall engage an independent IT security assessment / Penetration Test of the IT infrastructure including Disaster Recovery sites. This must be undertaken at least annually to identify vulnerabilities that could be exploited to breach the privacy of Barclays Data through Cyber Attacks. All vulnerabilities must be prioritised and tracked to resolution. The test must be undertaken in line with Good Industry Practice and by a recognised Security Assessment Vendor. • Supplier shall inform and agree on scope of security assessment with Barclays and test activities, in particular start and end date/times to allow any events raised by Barclays monitoring systems. Also, to prevent disruption to key Barclays activities such as end of year finance reports etc. • Barclays and/or its Agents shall have the right to conduct a Security Assessment of the Supplier Systems subject to 20 Business Days written notice from Barclays to the Supplier. The frequency, scope and methods used to conduct the Security Assessment shall be communicated to the Supplier 15 Business Days prior to commencement of the Security Assessment. • Any or all issues the Supplier has decided to risk accept must be communicated and agreed with Barclays.

Security Assessment means tests performed on the Supplier Systems in order to:

a) identify design and/or functionality issues in applications or infrastructure;
b) probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures;
c) identify potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws including, but not limited to, the following examples for infrastructure and application testing which could expose the Supplier and Barclays to risks from malicious activities;
   i. invalidated or unsanitised input;
   ii. broken access control;
   iii. broken authentication and session management;
   iv. cross-site scripting (XSS) flaws;
   v.
   vi. buffer overflows;
   vii. injection flaws;
   viii. improper error handling;
   ix. insecure storage;
   x. denial of service;
   xi. insecure configuration management;
   xii. proper use of SSL/TLS;
   xiii. proper use of encryption; and
   xiv. anti-virus reliability and testing,

This assessment will typically incorporate activities also commonly referred to as penetration testing.

Security Assessment Vendor means a suitably qualified Third Party employed to perform a Security Assessment.

9. System Configuration – Minimum Control Requirements

Control Area	Control Title	Control Description
System Configuration	System Time	All devices and systems must have correct and consistent time at all times to prevent system errors and also to ensure activities can be forensically investigated. Acceptable mechanism to ensure a consistent time that would meet forensic rigour. For example, are we recommending that they synchronize to 3 or 4 stratum 2 NTP servers and take the average, or synchronize with 2 approved stratum 1 servers.
System Configuration	Remote Access	All remote access to systems must be authorised and approved by Barclays prior to access being established to prevent security breaches. Remote access must be via multi factor authentication. User activity shall be logged and subject to review.
System Configuration	Secure Build	Host systems and network devices forming part of the Supplier Systems must be configured to function in accordance with Good Industry Practice, applicable specifications and functionality requirements to prevent unauthorised or incorrect updates being applied to such systems and network devices

10. System Monitoring – Minimum Control Requirements

Control Area	Control Title	Control Description
System Monitoring	Log Management	All key systems including key applications must be set to log key events. Logs must be centralized, appropriately secured and kept for a minimum of 12 months. The key events must be those that have the potential to impact the confidentiality, integrity and availability of the Service to Barclays and that may assist in the identification or investigation of material incidents and/or breaches of access rights occurring in relation to the Supplier Systems. Supplier must inform Barclays on serious incidents such as loss of customer data or serious compromise of system. Is there regulatory requirements for reporting a breach The Supplier must record and monitor the following as a minimum: i. User identification ii. Type of event iii. Date and Time iv. Success or failure indication v. Origination of event vi. Identity or name of affected data, system component, or resource. vii. Administrator activities
System Monitoring	Log Review	Logs must be reviewed for potential Cyber Security breaches / fraudulent activity which must be in sync with NTP. Event data must be collected and correlated from multiple sources and sensors. Detected events must be analyzed to understand attack targets and methods. Upon identification of any material incidents and/or breaches of access rights shall ensure that the Incident Management Process is followed

11. Right of Inspection – Minimum Control Requirements

Control Area	Control Title	Control Description
Right of Inspection	Barclays Right of Inspection	Barclays may, upon giving not less than 10 Business Days written notice conduct a security review of any site being used by or required to be used by the Supplier or its Sub-contractors to develop, test, enhance, maintain or operate the Supplier Systems used in the provision or recovery of the Services in order to review the Supplier's compliance with its obligations. Barclays may also carry out an inspection immediately after a Security Incident. Any non-compliance identified by Barclays during an inspection shall be risk assessed by Barclays and Barclays shall specify a timeframe within which the Supplier shall complete any required remediation and the Supplier shall complete any required remediation within that timeframe. The Supplier shall provide all assistance reasonably requested by Barclays in relation to any inspection.

12. Bank Dedicated Space – Control Requirements (NB please check with your Sourcing rep if required)

Control Area	Control Title	Control Description
Bank Dedicated Space	Physical Separation	The physical area occupied must be dedicated to Barclays and not shared with other companies / vendors.
Bank Dedicated Space	Physical Access Control	Secure automatic controls must be operating for access to BDS including: 1) If for authorised staff; i) Photo ID badge which is visible at all times ii) proximity card readers are implemented iii) Anti-pass back mechanism is enabled 2) Visitor/vendor controls i) Sign in log book ii) Limited use badge which is visible at all times
Bank Dedicated Space	Physical Access Control	Alarms must be configured to report through a centralised access system with auditable access control
Bank Dedicated Space	Physical Access Control	Monitor the controls ensuring appropriate access is granted to the BDS and other critical areas
Bank Dedicated Space	House Keeping	Only authorised housekeeping and support staff like electricians, AC maintenance, house-keeping etc. must be allowed in the BDS
Bank Dedicated Space	Environmental Controls	Controls must be implemented to protect against environmental factors for example fire, flood, hurricane, tornado, pestilence, infestations, humidity, temperature, dust, food & drink contamination

Bank Dedicated Space	Media Handling	Access to all media pertaining or relating to the services delivered to Barclays must be strictly controlled and authorised
Bank Dedicated Space	Clean Room Controls (Wealth Data only)	Specific controls for Clean Room requirements only are implemented as advised by Wealth data privacy requirements.
Bank Dedicated Space	Remote Access - ID&V	Every individual user must only authenticate to the Barclays network from the BDS using a Barclays provided multi factor authentication token
Bank Dedicated Space	Remote Access - Software Tokens	Installation of any RSA software and soft tokens must be done by administrators within the approved BDS on desktops
Bank Dedicated Space	Remote Access - Out of Office Support	Remote access to BDS environment is not provided by default for out of office hours/out of business hours support. Any remote access must be approved by Barclays
Bank Dedicated Space	Email and Internet	Network connectivity must be securely configured to block email and internet activity on the vendor's network
Bank Dedicated Space	System and Desktops	Secure desktop builds must be configured to industry best practice for computers within the BDS
Bank Dedicated Space	System and Desktops	Generic or shared or privilege access accounts and printing must not be permitted from the Barclays hosted system within the BDS. Any additional applications or tools installed must not introduce security weaknesses
Bank Dedicated Space	System and Desktops	Patching and updating processes and procedures must be in place to cover automatic and manual patching
Bank Dedicated Space	Testing and development environment	Software development must only be performed for Barclays owned programs within the BDS
Bank Dedicated Space	Source Code	Source code must be securely executed, stored and sent to Barclays.

Bank Dedicated Space	Network Controls - Transmission	All the information must be transmitted securely between BDS environment and Barclays and the management of network devices must be done using secure protocols
Bank Dedicated Space	Network Controls - Routing	Routing configuration must ensure only connections to the Barclays network and must not route to any other networks
Bank Dedicated Space	Network Controls - Wireless	Wireless networks must not be used in the Barclays network segment to provision services.
Bank Dedicated Space	Network Segregation	There must be separate network segments (i.e. business processing / live system support / systems development)
Bank Dedicated Space	File Storage	All file storage must be within BDS environment
Bank Dedicated Space	Remote Access - Software Tokens	Installation of any RSA software and soft tokens must be done by administrators within the approved BDS on desktops
Bank Dedicated Space	Remote Access - Out of Office Support	Remote access to BDS environment is not provided by default for out of office hours/out of business hours support. Any remote access must be approved by Barclays
Bank Dedicated Space	Email and Internet	Network connectivity must be securely configured to block email and internet activity on the vendor's network
Bank Dedicated Space	System and Desktops	Secure desktop builds must be configured to industry best practice for computers within the BDS
Bank Dedicated Space	System and Desktops	Generic or shared or privilege access accounts and printing must not be permitted from the Barclays hosted system within the BDS. Any additional applications or tools installed must not introduce security weaknesses
Bank Dedicated Space	System and Desktops	Patching and updating processes and procedures must be in place to cover automatic and manual patching

Bank Dedicated Space	Testing and development environment	Software development must only be performed for Barclays owned programs within the BDS
Bank Dedicated Space	Source Code	Source code must be securely executed, stored and sent to Barclays.
Bank Dedicated Space	Network Controls - Transmission	All the information must be transmitted securely between BDS environment and Barclays and the management of network devices must be done using secure protocols
Bank Dedicated Space	Network Controls - Routing	Routing configuration must ensure only connections to the Barclays network and must not route to any other networks
Bank Dedicated Space	Network Controls - Wireless	Wireless networks must not be used in the Barclays network segment to provision services.
Bank Dedicated Space	Network Segregation	There must be separate network segments (i.e. business processing / live system support / systems development)
Bank Dedicated Space	File Storage	All file storage must be within BDS environment

13. Cryptography– Minimum Control Requirements

Control Area	Control Title	Control Description
Cryptography	Cryptographic Key Management	The Supplier shall ensure that where secret or private cryptographic keys are used to protect Barclays Data identity and/or reputation, the keys are managed securely throughout their lifetime, in accordance with documented control requirements and procedures which are consistent with Good Industry Practice, and shall ensure that the keys are protected against unauthorised access or destruction.
Cryptography	Cryptographic Key Management	The Supplier shall maintain a record of all cryptographic use, including all keys, certificates and cryptographic devices managed by the Supplier and be made available to Barclays upon request.
Cryptography	Public Key Infrastructure	The Supplier shall ensure that if public key infrastructure (PKI) is used or operated, it shall be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.
Cryptography	Public Key Infrastructure	The Supplier shall ensure that all digital certificates that represent Barclays are obtained directly from Barclays central certificate management function and the Supplier shall manage the lifecycle of the certificate to ensure continued validity.
Cryptography	Public Key Infrastructure	The Supplier shall ensure that where private cryptographic keys are used to protect Barclays Data, identity and/or reputation, that all keys are protected by a FIPS 140-2 Level 3 or above certified hardware security modules (HSMs).