Supplier Control Obligation (SCO)

Management Control Requirements –

Information, Cyber & Physical Security, Technology, Recovery Planning, Data Privacy, Data Management and EUDA

MC 1.0 – Governance and Accountability

The Supplier must have an established and consistent industry standard framework for Information Technology , Information Technology Security, Physical Security, Recovery Planning, Data Management and Personal Information Management (Data Privacy/Data Protection) governance (NIST, ISO/IEC 27001, COBIT, BS10012, SSAE 18, ITIL) or similar best industry practice standard framework, to ensure the safeguards or countermeasures of their process, technology and physical environment are attested to be operating effectively. A well-structured, enterprise-wide governance programme must ensure that the core concepts of availability, integrity and confidentiality are supported by adequate controls. The controls must be designed to mitigate or reduce the risks of loss, disruption or corruption of information and Supplier must ensure that Barclays requirement controls are applied and operating effectively to protect service(s) provided to Barclays.

A governance framework must be established, and it must include administrative, technical, and physical safeguards to protect assets and Information/data from accidental and/or deliberate loss, disclosure, alteration or destruction, theft, inappropriate use or misuse and unauthorized access, use or disclosure.

The governance and accountable programme must include, but not be limited to, the following areas:

- Policies for Governance - A set of policies for governance shall be defined, approved by management, published, and communicated to Supplier employees and relevant parties and maintained.
    - Policies, procedures, standard programme that effectively create, implement, and continuously measure the effectiveness of the policy and standards implementation.
    - A comprehensive governance programme with clear leadership structure and executive oversight to create a culture of accountability and awareness.
    - A continuous communication of approved policies and procedures across the organisation.
    - Adapting legal requirements into policies and practices, data protection by design, and other controls to ensure that policies and processes are effectively implemented
- The policies for all domain areas shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
    - Ensure that policies and procedures/standards are routinely reviewed (at least annually, or at the point of any material changes whichever early).
    - Appoint an experienced and suitably qualified individual or individuals/team with whom Barclays can liaise for SCO requirements including physical and building security, information and cyber security, and personal information management (data privacy/data protection), Recovery Planning, Data Management and who will be responsible for, Barclays or Supplier control requirements are effectively implemented and monitored.

    - The Supplier must coordinate and align roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of controls with internal and sub-contractors/sub-processors.
- The Supplier must implement a secure infrastructure and control framework to protect the organisation from any threats (including Cyber Security)
- The Supplier shall set an independent audit program to examine whether Supplier controls are implemented, maintained, and must be performed at least annually.

Guidance for Cloud Service Customer (Supplier)

An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. The cloud service customer's information security policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for its information and other assets. When defining the information security policy for cloud computing, the cloud service customer should take the following into account:

- Information stored in the cloud computing environment can be subject to access and management by the cloud service provider.
- Assets can be maintained in the cloud computing environment, e.g., application program.
- Processes can run on a multi-tenant, virtualized cloud service.
- The cloud service users and the context in which they use the cloud service.
- The cloud service administrators with privileged access to the cloud service customer.
- The geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data (including temporary storage).

The relevant Security Policy of the cloud service customer should identify the cloud service provider as a type of Supplier and manage them in accordance with the security policy. This should aim to mitigate risks introduced by access and management of cloud service customer's data associated with cloud service provider.

The cloud service customer should consider relevant laws and regulations of jurisdictions governing the cloud service provider, in addition to those governing the cloud service customer. The cloud service customer should obtain evidence of the cloud service provider's compliance with relevant regulations and standards required for the cloud service customer's business. Such evidence can also be the attestations/certificates produced by third-party auditors.

The Supplier must notify Barclays in writing as soon as they are legally able to do so if the Supplier is subject to a merger, acquisition, or any other change of ownership.

MC 2.0 - Risk Management

The Supplier must establish a risk management programme that effectively evaluates, mitigates, and monitors risks across the Supplier controlled environment.

The risk management programme must include, but not be limited to, the following areas:

- The Supplier must have an appropriately approved risk management framework (e.g., Personal Information if processing PI data, Information, Cyber, Physical, Technology, Data & Recovery Planning) and able to demonstrate its incorporation into the business strategy
- Aligned with the risk framework, formal risk assessments must be performed at least annually or at planned intervals, using a risk-based approach, or be triggered on an event driven basis e.g., in response to an incident or associated lessons learnt, in conjunction with any changes to information systems or physical building or space) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).
- Establishes and maintains risk criteria that include:
    - the risk acceptance criteria, and
    - criteria for performing risk assessments,
- Identifies the risks:
    - apply the risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the risk framework, and
    - identify the risk owners,
- Analyses the risks:
    - assess the potential consequences that would result if the risks identified,
    - assess the realistic likelihood of the occurrence of the risks identified, and
    - determine the levels of risk
- Evaluates the risks:
    - compare the results of risk analysis with the risk criteria established, and
    - prioritise the analysed risks for risk treatment
- Risk treatment:
    - select appropriate risk treatment options, taking account of the risk assessment results,
    - determine all controls that are necessary to implement the risk treatment option(s) chosen,
    - produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and

        - The Supplier must ensure that identified risks are minimized or eliminated in the environment through the prioritisation of risk and implementation of countermeasures. The Supplier should continually monitor the countermeasures for them to be effective.
- Supplier must perform as a minimum an annual risk assessment in relation to Information, Cyber, Physical Security, Personal Information Management (Data Privacy/Data Protection) and Recovery Planning. Based on the specific environments with current and emerging threats, Supplier must consider a more frequent cadence.
    - Asses at least annually the sites critical to the operation of processes/services provided to Barclays (including Data Centres)
- The organisation shall retain documented information about the information security risk assessment process.
- Risk assessments associated with data governance requirements (including Personal Information if processing PI data) must consider the following:
    - Data classification and protection from unauthorized use, access, loss, destruction, and falsification.
    - Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure.
    - Compliance with defined retention periods and end-of-life disposal requirements.
- Supplier while acting as a controller or a processer must assess possible privacy risk when processing sensitive or large volumes of Barclays data to ensure any changes in their handling/processing of Barclays data don't result in a privacy risk
- Supplier must develop and implement the organisational governance structure to enable an ongoing understanding of the organisation risk management priorities informed by privacy risk

MC 3.0 - Roles and Responsibilities

The Supplier is responsible for ensuring that all its employees including but not limited to contractors, sub-contractors, sub-processors involved in providing service to Barclays are aware of and adhere to Barclays control requirements. The Supplier must ensure that a suitable team of specialists and/or individuals with commensurate and appropriate skills, defined roles, and responsibilities to support and/or manage Barclays control requirements are placed to operate effectively for the protection of Barclays services(s).

The Supplier must define and communicate roles and responsibilities to effectively support the Barclays control requirements. The roles & responsibilities must be reviewed regularly (and in any event not less than once every 12 months) and after any material change to the Supplier operating model or business.

It is the responsibility of the Supplier to ensure that their employees, contractors, sub-contractors/sub-processors are familiar and conform to the control requirements of this standard and associated policies and standard. The Supplier must appoint a Point of Contact to liaise with Barclays for any escalation arising out of non-compliance to the Control Requirements. Specific contractual requirements must be flowed down in writing to the Supplier subcontractors/ sub-processors.

Guidance for Cloud Service Customer (Supplier)

The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities and confirm that it can fulfil its allocated roles and responsibilities. The roles and responsibilities of both parties should be stated in an agreement. The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.

The cloud service customer should define or extend its existing policies and procedures in accordance with its use of cloud services and educate its cloud service users of their roles and responsibilities in the use of the cloud service.

MC 4.0 - Education and Awareness

The Supplier must run on a continual basis an awareness training programme for all Supplier employees including contractors, short term hires and consultants. All the Supplier employees working for Barclays services and/or access to Barclays data/ information or other physical assets must receive appropriate training and regular awareness updates in organisational policies, processes and procedures relating to their professional function within the organisation. The levels of training and awareness must prepare the Supplier employees to perform their roles securely and ensure that the Supplier employees understand their responsibilities while accessing or processing any Barclays data including any personal data. The records of the programme being undertaken must be recorded in a suitable learning management platform or through manual process.

The Supplier must ensure that all Supplier employees complete mandatory education and awareness training, which shall include Cyber Security, Physical Security, Recovery Planning, Personal Information Management (Data Privacy/Data Protection), Data Management, IT service management, EUDA and protection of Barclays data within **one month of joining** the organisation and/or upon joining Barclays service(s). Besides refreshing training annually, the Supplier must ensure to test to verify that the Supplier employees understand their responsibilities and are aware of risks associated with the Barclays data, applicable laws, and regulations as well as other factors that could affect performance or pose risk to bank. All training delivered must be recorded and maintained for all Supplier employees working on Barclays service(s) and produced for inspection by Barclays when requested.

The Supplier must ensure that their awareness training programme includes following Cyber security topics - social engineering and insider threat, it is recommended that the Supplier performs simulation tests on social engineering attacks using techniques such as Phishing Simulations tests for all employees at an enterprise level with ongoing monitoring to ensure that the threat of such risks is clearly understood and mitigate identified issues.

High-risk groups, such as those with access to privileged system(s), access to high risk or critical space or in sensitive business functions (including privileged users including developers and support, senior executives, Information security personnel and third-party stakeholders), must receive Information security and physical security situational awareness training according to their roles and responsibilities.

All Physical Security personnel (whether employed by the Supplier, a property owner or an external Supplier must be engaged or contracted through an accredited, licensed service provider in accordance with local legislation, and where required by jurisdiction, be personally licensed to undertake security duties. Physical Security Personnel must receive security training commensurate with their role and responsibilities. All training delivered must be documented and a training record must be maintained for all security personnel and produced for inspection by Barclays when requested

Supplier must ensure that its third-party personnel with access to data containing any personal information are aware of privacy risks and perform their duties and responsibilities consistent with related policies, processes, procedures, agreements, and organisational privacy values. All training delivered must be documented and a training record must be maintained for all personnel and produced for inspection by Barclays when requested.

Supplier must train employees to effectively perform their duties in data management (managing critical data elements or third party managed applications).

Supplier EUDA owner must identify Supplier employees with EUDA responsibilities and ensure that they complete the education and awareness training appropriate to their role at least once per year and retain evidence that must demonstrate the conformance to control.

Guidance for Cloud Service Customer (Supplier)

The cloud service customer should add the following items to awareness, education and training programme for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including relevant employees and contractors:

- Standards and procedures for the use of cloud services.
- Information security risks relating to cloud services and how those risks are managed.
- System and network environment risks with the use of cloud services.
- Applicable legal and regulatory considerations.

Information security awareness, education and training programme about cloud services should be provided to management and the supervising managers, including those of business units. These efforts support effective co-ordination of information security activities.

MC 5.0 - Incident Management

The Supplier must have an established Incident Management framework that effectively manages, contains, and removes /mitigates an incident and its underlying cause from the Supplier environment.

The Supplier must have an Incident and Crisis Management procedure which includes the process for escalating Incidents/Crises to Barclays. The Supplier must ensure that Incident/Crisis response teams and processes are tested, at least annually, to demonstrate that the Supplier is able to respond to any Incidents effectively and efficiently. The Supplier must also test their ability to notify within defined timelines to appropriate contacts, of an incident and demonstrate to Barclays when requested to do so.

The Supplier must have a well-documented Incident response plan that defines roles of Supplier employees as well as the phases of incident handling/management:

- Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to incidents.
- Reporting incident events – Incident events shall be reported through appropriate management channels as quickly as possible and reporting mechanism must be as easily, accessible to all Supplier employees and contractors.
- Assessment of incident events – Incident events must be assessed to determine appropriate criticality, classification and response required.
    - Incident Classification - Establish an incident classification scale and decide whether the event must be classified as incident. Classification and prioritisation of incidents can help to identify the impact and extent of an incident.
- Response to Incidents - Incidents shall be responded to in accordance with the Supplier Incident Management documented procedures.
    - Incident Containment - Utilise people, process, and technology capabilities to quickly and effectively contain an incident in the environment.
    - Threat Removal/ Mitigation - Leverage people, process, and technology capabilities to quickly and effectively remove/ mitigate a security threat and/or its components from the environment.
- Learning from incidents - Knowledge gained from analysing and resolving incidents shall be used to reduce the likelihood or impact of future incidents.
- Collection of evidence - The Supplier shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

Post Incident - Following a disruption to the Barclays service(s), a Post Incident Report must be provided to Barclays within a maximum Four calendar weeks of the reinstatement of the service to normal operating levels. Minimum requirement of Post Incident Report:

- The events surrounding the situation.
- How the Incident/Crisis was managed.

- Analysis of its root cause.
- Whether it is classed as a 'Risk Event' by Supplier or Barclays (i.e., deemed sufficiently significant that it must be notified/escalated to relevant stakeholders in accordance with the applicable policies known to Supplier).
- Whether it represents a 'Conduct Risk' (e.g., if Supplier is dealing directly with Barclays' customers).
- Any Barclays' customer-redress known to Supplier,
- Continuous improvement to prevent reoccurrence, and
- Supplier must seek to establish that response activities are improved where possible by incorporating lessons learned from current and previous detection/response activities.

For Communication –Supplier must appoint a Point of Contact who will liaise with Barclays in the event of an incident/crisis. The Supplier must notify Barclays of the individual(s) contact details and any changes to them, including any out of hours' contacts and telephone numbers.

Details must include: -Name, responsibilities within the organisation, role, email address and telephone number

If at any time Supplier confirms that any incident impacts Barclays Services, Barclays Systems or Barclays Data, Supplier shall notify Barclays immediately.

Upon Supplier becoming aware of a Cyber Incident, including by notification from a Barclays Entity, Supplier shall immediately, but in no event later than required by Applicable Law or, if no such requirement, within 48 hours after first becoming aware of the Cyber Incident, notify Barclays by sending an email to gcsojoc@barclays.com, and provide all relevant information, including, if possible (a) the categories and approximate number of affected Barclays data records, and, if applicable, the categories and approximate number of affected data subjects; (b) the impact and likely consequences of the Cyber Incident to Barclays and, if applicable, the affected data subjects; and (c) the corrective and mitigating actions taken or to be taken by Supplier.

In the event of any actual, suspected or alleged theft, unauthorized use or disclosure of any Protected Personal Data due to a failure of the security safeguards of Supplier (or any Supplier Personnel) or unauthorized access to Protected Personal Data from or through Supplier (or any Supplier Personnel), or loss, damage or destruction of Protected Personal Data in Supplier or any Supplier Personnel's possession or control, or other unauthorized Processing of any Protected Personal Data, Supplier shall notify Barclays as soon as practicable, and in any event within 24 hours after becoming aware of the relevant event, by sending an email to gcsojoc@barclays.com, and provide full cooperation and assistance to Barclays in respect of such event, including providing all relevant information such as data, time, location, type of incident, impact, status, and mitigation actions taken.

If a subcontractor/sub-processor is used to provide the service, where they will hold or process Barclays Data/ Information or assets, the Supplier must obtain agreement from Barclays. Supplier must have a contractual relationship with the sub-contractors/sub-processors and must ensure the sub-contractors/sub-processors is accredited with similar best industry practice standard framework operating effectively

to protect Barclays data/information they process and/or hold. In case of incident with subcontractor/sub-processor must ensure above incident, notification must be followed.

Guidance for Cloud Service Customer (Supplier)

The cloud service customer should verify the allocation of responsibilities for Incident Management and should ensure that it meets the requirements of the cloud service customer. The cloud service customer should request information from the cloud service provider about the mechanisms for:
– the cloud service customer to report an incident/event it has detected to the cloud service provider.
– the cloud service customer to receive reports regarding an incident/ event detected by the cloud service provider.
– the cloud service customer to track the status of a reported information security event.

MC 6.0 – IT Asset Management (Hardware & Software)

The Supplier must have and operate an effective asset management programme throughout the asset lifecycle. Asset management must govern the lifecycle of assets from acquisition to retirement and/or secure disposal, providing visibility and security to all asset classes in the environment.

The Supplier must maintain a complete, accurate and up to date inventory of business-critical assets located at all sites and/or geographical locations in scope of service(s) to Barclays, including any Barclays equipment hosted in Supplier premises, a sub-contractors/sub-processors provided by Barclays, and ensure that there is at least one test annually to validate that the Information asset inventory is current, complete and accurate and demonstrate the results to Barclays when requested.

Asset Management process must cover the following areas:

- Inventory of assets - Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
    - Supplier must maintain an accurate and up-to-date inventory of all IT hardware assets with the potential to store or process information.
    - Supplier must have an accurate and up to date information asset inventory for Barclays equipment hosted in Supplier and/or Barclays IT assets provided to Supplier.
    - Supplier with a Tier1, Tier 2 and Tier 3 setup must maintain current, complete, and accurate asset inventories (including, desktops, laptops, network equipment, RSA tokens or any Barclays provided assets).
    - Supplier must perform reconciliation of all the Barclays assets (Hardware & Software) on annual basis and inform Barclays (Chief Security Office- TPSecM Team) of its results.

  - Maintain an up-to-date inventory of all deployed, authorised software products required for Barclays service delivery and comply to terms and conditions of the respective licenses.
  - The cloud service customer's inventory of assets must account for information and associated assets stored in the cloud computing environment. The records of the inventory must indicate where the assets are maintained, e.g., identification of the cloud service.
- Acceptable use of assets - Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented.
  - Ensure that unauthorised assets are either removed from the network.
  - The Supplier must ensure effective and efficient procedures are implemented for the mitigation of un-supported technologies and the end-of-life, retirement, and secure disposal of assets and data to eliminate the risk
  - Tag Unsupported software and hardware as unsupported in the inventory system.
- Return of assets - All Supplier employees and sub-contractors/sub-processors (in scope of service(s) to Barclays) shall return all the Barclays assets in their possession upon termination of their employment, contract, or agreement.
  - Barclays assets 'Lost or Stolen' must be properly investigated and reported to Barclays in accordance with incident management control.
  - In cases of 'Lost or Stolen' of Supplier assets contains Barclays Information needs to be reported to Barclays in accordance with incident management control.

The Supplier must promptly advise Barclays of known changes in their capability to support, whether directly or indirectly, for IT assets used in the provision of services to Barclays including where products have security vulnerabilities and must ensure timely upgrade or retirement of those IT assets.

Barclays Asset Transportation - Supplier will ensure that all Barclays assets and Barclays Data are transported securely with proportionate controls commensurate to the classification and value of the assets and data being moved (both from a financial and reputational damage perspective) incorporating impact of the threat environment in which they are being transported.

Support Management (Supplier)

The Supplier must promptly advise Barclays of known changes in their capability to support, whether directly or indirectly, for IT assets used in the provision of services to Barclays including where products have security vulnerabilities and must ensure timely upgrade or retirement of those IT assets.

The Supplier must ensure that any potential changes in key third party support arrangements are identified and communicated to Barclays for the affected assets in order to ensure that the Product information is kept up-to date.

Guidance for Cloud Service Customer (Supplier)

The cloud service customer's inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should indicate where the assets are maintained, e.g., identification of the cloud service.

Installing commercially licensed software in a cloud service can cause a breach of the license terms for the software. The cloud service customer should have a procedure for identifying cloud-specific licensing requirements before permitting any licensed software to be installed in a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable, and the software can be run on more systems or processor cores than is permitted by the license terms.

MC 7.0 – Secure Disposal/Destruction of Physical Assets and Data Remanence of Electronic Information

Secure destruction or erasure of Barclays Information Assets including images used for service, stored in either physical and/or electronic form, must be performed in an appropriate secure method and verify that Barclays data is not recoverable.

The Supplier must establish procedures with supporting business processes and technical measures to securely dispose using appropriate santisation methods including but not limited to clearing, purging, and destroying for secure removal/erasure and recovery of Barclays data from all storage media rendering Barclays data irrecoverable by known computer forensic means.

Barclays data stored in media must be wiped to render the data irrecoverable using appropriate data erase techniques like secure wipe, purging, data clearing, or asset destruction or software-based method to overwriting the data or use the industry standard framework on data disposal (NIST). All equipment (Information Assets) must be disposed of at the end of its life and/or operational life (faulty, decommissioned due to service retired or no longer required, used in a trial or proof of concept, Data erasure services can be utilised for equipment that is to be reused, etc.).

Disposal requirements apply to Supplier sub-contractors/sub-processors that are used to provide the service to Barclays.

Dispose of hardcopy information must be shredded to a minimum of P4 DIN66399 standard using a crosscut shredder (this includes Payment Card information) or may be incinerated in compliance with BS EN15713:2009.

For Barclays, evidence of data disposal must be kept, providing audit trail, evidence and tracking and must include:

- Proof of destruction and/or disposal (including date undertaken and method used)
- System audit logs for deletion.
- Data disposal certificates.
- Who undertook the disposal (including any disposal partners / 3rd party's or contractors)?
- A destruction and verification report must be generated to confirm the success or failure of any destruction / deletion process. (i.e., an overwriting process must provide a report that details any sectors that couldn't be erased).

During the exit from service to Barclays, the Supplier must ensure Barclays data is securely destroyed upon notification and authorisation from Barclays.

Guidance for Cloud Service Customer (Supplier)

The cloud service customer should request confirmation that the cloud service provider has the policies and procedures for secure disposal or reuse of resources. The cloud service customer should request a documented description of the termination of service process that covers return and removal of cloud service customer's assets followed by the deletion of all copies of those assets from the cloud service provider's systems. The description should list all the assets and document the schedule for the termination of service, which should occur in a timely manner.

MC 8.0 – Information Classification and Data Handling

The Supplier must have an established and appropriate information classification and data handling framework/scheme (aligned to Good Industry Practice and/or Barclays requirements) covering the following components:

- Classification of information - Information shall be classified in terms of criticality and sensitivity to unauthorised disclosure or modification.
- Labelling of information - An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the Supplier.
- Handling of assets - Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the Supplier.

The Supplier must also ensure that all staff are aware of the Supplier/Barclays Labelling and handling requirements and how to correctly apply the correct information classification.

The Supplier must refer to the Barclays Information Labelling Schema and handling requirements (Appendix A, Table A1 and A2), or an alternative scheme to ensure that Supplier protects and secures the Barclays Information held and/or processed. This requirement applies to all Barclays Information Assets held or processed on behalf of Barclays including sub-contractors/sub-processors.

Guidance for Cloud Service Customer (Supplier)

The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the cloud service customer's adopted procedures for labelling. Where applicable, functionality provided by the cloud service provider that supports labelling can be adopted.

MC 9.0 Information/ Data Backup

The Supplier must have an established Data Backup process to ensure that infrastructure is regularly and accurately backed up in order to prevent the loss of data. Information stored in an electronic form is backed up to keep it safe in the event of system failure, disasters, or incident. Backup plans should be developed, tested, and implemented to address the topic-specific policy on backup.

Backup plan, the following items should be taken into consideration:

- Determining backup requirements - Requirements for data backup are clearly defined, recorded, and agreed with the business
- Producing accurate and complete records of the backup copies and documented restoration procedures.
- Backup frequency (e.g., full, or differential backup)
- Safe storage of backups
    - storing the backups in a safe and secure remote location, at a sufficient distance to escape any damage from a disaster at the main site.
- Regularly testing backup media to ensure that they can be relied on for emergency use when necessary. Testing the ability to restore backed-up data onto a test system, not by overwriting the original storage media in case the backup or restoration process fails and causes irreparable data damage or loss.
- Taking care to ensure that inadvertent data loss is detected before backup is taken.
- Validate the backup is fit for purpose

Ensure that backups are properly protected via physical security and/or encryption when they are stored, as well as when they are moved across the network/locations. This includes remote backups and cloud services.

Ensure that all Barclays data is backed up on a regular basis as per the service requirement.

Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service customer should also verify that they meet their backup requirements. The cloud service customer is responsible for implementing backup capabilities when the cloud service provider does not provide them.

The Supplier must ensure that all IT systems and services used in the provision of services to Barclays have adequate backup and restore processes in place that are operating in line with Barclays' needs and are periodically proven to be effective.

The Supplier must ensure that all backup media associated with the provision of services to Barclays, together with the arrangements for the handling and storage of those media, remain secure and reliable at all times

MC 10.0 Configuration Management

The Supplier should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (including cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.

Managing configurations – The Supplier should have a set of approved and tested configurations for hardware, software, and networks. These should be recorded, and a log should be maintained of all configuration changes. These records should be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

Monitoring configurations - Configurations should be monitored with a comprehensive set of system management tools (e.g., maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths, and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

Recording & Maintaining Configuration Items - The Supplier must maintain a complete and accurate register entry for all in-scope Configuration Items used in the provision of services to Barclays (including ownership and upstream/downstream dependencies/mappings). The Supplier must have controls in place that assure the ongoing maintenance of the accuracy and completeness of the data.

Isolating the Production Environment - The Supplier must ensure that production services provided to Barclays have no dependencies on any non-production components, so that insecure or unreliable service delivery may be avoided.

Secure Configuration - The Supplier must have an established framework to ensure that all configurable systems and/or networking equipment are securely configured in accordance with Best Industry Practice (e.g., NIST, SANS, CIS).

- Establishes policies, procedures / organisational measures, and tools to allow for implementation of Best Industry Practice security configuration standards for all authorized network devices and operating Systems, applications, and servers.
- Performs regular (annual at a minimum) enforcement checks to ensure that non-conformance with baseline security standards is promptly rectified. Appropriate checks and monitoring are put in place to ensure the integrity of the builds / devices.

- Systems and network devices are configured to function in accordance with security principles (e.g., concept of limiting controls of ports, protocols and services, no unauthorised software, removing and disabling unnecessary user accounts, changing default account passwords, removing unnecessary software, etc.).
- Conduct periodic configuration audit at least annually to ensure actual production environment does not have any unauthorized configuration.
- Ensure configuration management governs secure configuration standards across all asset classes, and detects, alerts, and effectively responds to configuration changes or deviations.

Guidance for Cloud Service customer (Supplier) used for providing service(s) to Barclays

The Cloud Service Customer (CSC) must ensure that appropriate Secure Configuration controls are implemented to safeguard Barclays service -

- When configuring virtual machines, cloud service customers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.

MC 11.0 Artificial Intelligence (AI) Security requirements

The Supplier must consult with Barclays (Chief Security Office - TPSecM team (externalcyberassurance@barclayscorp.com) if they are using AI tools for any part of the lifecycle of services and/or processing Barclays data.

The Supplier must, where using AI for any part of the lifecycle of services and/or processing Barclays data, operate an AI Management System this Management System should at a minimum document processes/procedures around the following Points:

- AI Governance – The Supplier should define and establish a governance framework for usage of AI tools (including Third Party AI tools). This governance framework should ensure that AI tools are designed/deployed or integrated into existing processes in a manner which safeguards against data loss, system damage, service interruptions, and regulatory consequences. A well-structured, governance programme must ensure that the core concepts of availability, integrity and confidentiality are supported by adequate controls. The controls must be designed to mitigate or reduce the risks of loss, disruption, or corruption of information through the AI System and Supplier must ensure that security controls are applied and operating effectively to protect Barclays data and service(s) provided to Barclays where they are interacting with such AI System.

- AI Security - The Supplier must define and establish an AI security framework which should include, but not be limited to, the following areas:

- Policies related to AI – Supplier should document an AI policy which details requirements for the safe and responsible use or development of AI Systems
- Internal organisation – Supplier should ensure to establish accountability within the organisation to uphold its responsible approach for the implementation, operation, and management of AI systems.
- Resources for AI systems – Supplier should ensure that the organisation accounts for the resources (including AI system components and assets) of the AI system in order to fully understand and address risks and impacts.
- Data for AI systems – The Supplier must ensure that the organisation understands the role and impacts of data (including Barclays Data) in AI systems in the application and development, provision, or use of AI systems throughout their life cycles.
- Information for interested parties of AI systems – The Supplier to ensure that any relevant interested parties (including Barclays) have the necessary information to understand and assess the risks of the AI System and their impacts (both positive and negative).
- Third-party and customer relationships – The Supplier to ensure that the organisation understands its responsibilities and remains accountable in respect of the AI System and risks are appropriately apportioned when third parties are involved at any stage of the AI system life cycle.

EUDA - Where Supplier services or Supplier product capability or functionality delivered to Barclays uses EUDAs and AI is implemented or deployed to implement or support these EUDAs, Supplier must inform Barclays and ensure that AI usage does not conflict with Barclays EUDA SCO requirements.

Note: The above security control requirement is not only applicable for Artificial intelligence (AI), but also for Machine learning (ML), as Artificial intelligence and machine learning are very closely related and connected. The Supplier must implement all the above control requirements for using ML tools for any part of the lifecycle of services and/or processing Barclays data.

AI/ML Definition: AI means a machine-based system that is designed to operate with a level of autonomy and is capable, for a given set of objectives, of generating outputs such as predictions, recommendations or decisions that influence physical or virtual environments. ML is a subset of AI, which refers to the capability of a machine to improve its own performance from experience through iterations without being explicitly programmed with rules.

A method/application/tool that falls under above definition is considered as AI/ML if it demonstrates AI/ML characteristics[1] or uses a listed AI/ML algorithm[2].

1. A method/application/tool has AI/ML characteristics if it contains parameters that are trained on data, and the appropriateness of those parameters cannot be assessed individually by a subject matter expert. This may be due to the high number of parameters, complexity of the calculation, or the frequency with which they are updated. For purposes of this definition, "parameters" means numerical variables in the algorithm

which can be varied to affect its output; "appropriateness" means the output of the model is fit for purpose given its use; and "subject matter expert" means either model owner or model developer (if acts as a delegate for model development).

2. AI/ML algorithms include Bagging (random forest, etc.), Boosting (GBM, XGBoost, etc.), Clustering (K-means, DBSCAN, etc.), Deep learning/neural network, Instance-based learning (KNN etc.), Regularized regression (e.g., Lasso, ridge), Reinforcement learning, Support vector machine.

Right of Inspection

The Supplier must allow Barclays, upon Barclays giving not less than ten (10) Business Days written notice, to conduct a security review of any site or technology used by the Supplier or its Sub-contractors/Sub-processors to develop, test, enhance, maintain or operate the Supplier Systems used in the Services, in order to review the Supplier compliance with its obligations to Barclays. The Supplier must also allow Barclays to carry out an inspection on at least an annual basis and/or immediately after a security incident.

Any non-conformance to controls identified by Barclays during an inspection must be risk assessed by Barclays and Barclays must specify a remediation timeframe. The Supplier must then complete any required remediation within that timeframe.

The Supplier must provide all assistance reasonably requested by Barclays in relation to any inspection and documentation submitted during inspection. The documentation needs to be completed and returned back to Barclays promptly. Supplier also must support Barclays with assessment questioner along with evidence requested during any assurance review. Each Party shall bear its own costs with respect to any review/audit/assessment.

Appendix A: Barclays Information Labelling Schema and Data Handling Requirements

Table A1: Barclays Information Labelling Schema

Label	Definition	Examples
Secret	Information must be classified as **Secret** if its unauthorised disclosure would have an adverse impact on Barclays, assessed under the Enterprise Risk Management Framework (ERMF) as "Critical" (financial or non-financial). This information is restricted to a specific audience and must not be distributed further without the originator's permission. The audience may include external recipients at the explicit authorisation of the information owner.	• Information on potential mergers or acquisitions • Strategic planning information – business and organisational • Certain information security configuration information • Certain audit findings and reports • Executive committee minutes • Authentication or Identification & Verification (ID&V) details – customer/client & colleague • Bulk volumes of cardholder Information • Profit forecasts or annual financial results (prior to public release) • Any items covered under a formal Non-Disclosure Agreement (NDA)
Restricted - Internal	Information must be classified as **Restricted - Internal** if the expected recipients are only Barclays authenticated employees and Barclays Managed Service Providers (MSPs) with an active contract in place and which is restricted to a specific audience. Unauthorised disclosure would have an adverse impact on Barclays, assessed under the ERMF as "Major" or "Limited"(financial or non-financial). This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	• Strategies and budgets • Performance appraisals • Staff remuneration and personal data • Vulnerability assessments
Restricted - External	Information must be classified as **Restricted - External** if the expected recipients are Barclays authenticated employees and Barclays MSPs with an active contract in place and which is restricted to a specific audience or external parties that are authorised by the information owner. Unauthorised disclosure would have an adverse impact on Barclays, assessed under the ERMF as "Major" or "Limited" (financial or non-financial). This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	• New product plans • Client contracts • Legal contracts • Individual/low volume customer/client Information intended to be sent externally • Customer/client communications. • New issue offering materials (e.g., prospectus, offering memo) • Final research documents

		• Non-Barclays Material Non-Public Information (MNPI) • All research reports • Certain marketing materials • Market commentary • Audit findings and report
Unrestricted	Information must be classified as Unrestricted if it is either intended for general distribution or would not have any negative impact on the organisation if it were to be distributed.	• Marketing materials • Publications • Public announcements • Job advertisements • Information with no impact to Barclays

Table A2: Barclays Information Labelling Schema – Data Handling Requirements

*** System security configuration Information, audit findings, and personal records may be classed as either Restricted – Internal or Secret, depending on the impact of unauthorised disclosure to the business

Lifecycle Stage	Secret	Restricted – Internal	Restricted – External
Create and introduce	• Assets must be assigned an Information Owner.	• Assets must be assigned an Information Owner.	• Assets must be assigned an Information Owner.
Store	• Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them. • Electronic assets in storage must be protected through encryption or appropriate compensating controls if there is a significant risk that unauthorised people may be able to access them. • All private keys that are used to protect Barclays Data, identity and/or reputation, must be protected by a FIPS 140-2 Level 3 or above certified hardware security modules (HSMs).	• Assets (whether physical or electronic) must not be stored in public areas (including public areas within the premises where visitors may have unsupervised access). • Information must not be left in public areas within premises where visitors may have unsupervised access.	• Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them. • Electronic assets in storage must be protected through encryption or appropriate compensating controls if there is a significant risk that unauthorised people may be able to access them.

Access & Use	• Assets (whether physical or electronic) must not be worked on or left unattended where unauthorised people may be able to view or access them. Assets may be worked on if suitable controls are in place (e.g., privacy screens). • Printed assets must be printed using secure printing tools. • Electronic assets must be protected by appropriate Logical Access Management controls	• Assets (whether physical or electronic) must not be left in public areas outside the premises. • Assets (whether physical or electronic) must not be left in public areas within the premises where visitors may have unsupervised access. • Electronic assets must be protected by appropriate Logical Access Management controls if required	• Assets (whether physical or electronic) must not be worked on or left unattended where unauthorised people may be able to view or access them. Assets may be worked on if suitable controls are in place (e.g., privacy screens). • Printed assets must be retrieved immediately from the printer. If this is not possible, secure printing tools must be used. • Electronic assets must be protected by appropriate Logical Access Management controls.
Share	• Hard copy assets must carry a visible Information label on every page. • Envelopes containing hard copy assets must carry a visible Information label on the front and be sealed with a tamper-evident seal. They must be placed inside an unlabelled secondary envelope prior to distribution. • Electronic assets must carry an obvious Information label. Electronic copies of multi-page documents must carry a visible Information label on every page. • Assets must only be distributed using systems, methods, or Supplier approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation. • Assets must only be distributed to people specifically authorised to receive them by the Information Owner. • Assets must not be faxed.	• Hard copy assets must be given a visible Information label. The label must be on the title page at a minimum. • Electronic assets must carry an obvious Information label. • Assets must only be distributed using systems, methods, or Supplier approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation.	• Hard copy assets must carry a visible Information label. The label must be on the title page at a minimum. • Envelopes containing hard copy assets must carry a visible Information label on the front • Electronic assets must carry an obvious Information label. Electronic copies of multi-page documents must carry a visible Information label on every page. • Assets must only be distributed using systems, methods, or Supplier approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation. • Assets must only be distributed to people with a business need to receive them. • Assets must not be faxed unless the sender has confirmed that the recipients are ready to retrieve the asset.

	• Electronic assets must be encrypted using an approved cryptographic protection mechanism when in transit outside the internal network. • A chain of custody for electronic assets must be maintained.		• Electronic assets must be encrypted using an approved cryptographic protection mechanism when in transit outside the internal network.
Archive and Dispose	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system "recycle bins" or similar facilities in a timely manner. • Media on which Secret electronic assets have been stored must be appropriately sanitised prior to, or during, disposal.	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system "recycle bins" or similar facilities in a timely manner	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system "recycle bins" or similar facilities in a timely manner.

Appendix B: Definitions

Barclays Confidential Information means any information obtained by Supplier Lead, Supplier or any Supplier Personnel (or to which any of them has access) in connection with these General Terms and/or any Contract that relates to any past, present or future (i) business activities, products and/or developments of any Barclays Entity and/or (ii) employees, customers, counterparties, Third Party/Suppliers and/or contractors of any Barclays Entity (other than Supplier Entities), including all intellectual property owned by any Barclays Entity (including pursuant to any Contract) or any such Third Party Supplier/contractor, Protected Personal Data, these General Terms, each Module and each Contract, and records maintained under any Contract and any information relating to the applicable entity's or person's plans, pricing, methodologies, processes, financial data, Intellectual Property Rights, research, systems, programme, and/or information technology;

Barclays Data means all data, information, text, drawings and other materials embodied in any medium including all electronic, optical, magnetic or tangible media that (i) are accessible by Supplier in connection with any Contract, (ii) are supplied to Supplier by any Barclays Entity, or (iii) Supplier generates, collects, processes, stores or transmits in connection with any Contract, excluding Supplier Materials.

Barclays Systems means the electronic information systems comprising any one or more of hardware, equipment, software, peripherals, and communications networks owned, controlled, operated and/or used by any Barclays Entity.

Cyber Incident means any event, whether such event has been confirmed to have actually occurred or if Supplier or Barclays has reasonable grounds to believe has occurred (based on a credible threat, intelligence or otherwise), that has resulted or has the potential to result in jeopardy to (i) the confidentiality, integrity or full availability of Barclays Data, or (ii) the confidentiality, integrity or full availability and normal operation of a Supplier System or a Barclays System.

Technology Incidents An unplanned interruption to an IT Service or a reduction in the quality of an IT Service, including, without limitation the failure of a Configuration Item that has not yet impacted a service. **Major Incident** - An Incident that poses a significant risk/impact to Barclays and can result in serious consequences including severe loss of productivity, reputational / regulatory damage and impact to core business processes, key controls, or systems.

Data Protection Impact Assessment means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by the Data Protection Legislation.

Data Protection Legislation means, to the extent applicable to the performance of any of Suppliers obligations under any Contract: (i) the EU Directive on Privacy and Electronic Communications 2002/58/EC (as may be modified or replaced from time to time), (ii) the EU General Data Protection Regulation 2016/679 (the **GDPR**), European Commission decisions and guidance and all national implementing legislation, (iii) the UK GDPR, (iv) Gramm–Leach–Bliley Act provisions relating to Non-public Personal Information, (v) the Health Insurance Portability and Accountability Act 1996, and (vi) all other applicable laws, regulations and regulatory guidance relating to data protection and privacy in (a) any jurisdiction in which the relevant Barclays Entity is located, Suppliers obligations are performed, the relevant Data Subject is located, or any Protected Personal Data is being Processed, stored or used and (b) any jurisdiction from which Supplier performs any of its obligations under any Contract;

Data Privacy Control Obligations means any data privacy schedule that forms a part of Schedule 7 (External Supplier Control Obligations).

Data Subject shall have the meaning given to it by the Data Protection Legislation. Where such term is not defined by the Data Protection Legislation, it shall mean an identified natural person or an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Good Industry Practice means, in relation to any undertaking and any circumstances, the exercise of the highest degree of skill, diligence, prudence and foresight that would reasonably be expected from a highly skilled and experienced person engaged in the same type of undertaking under the same or similar circumstances.

Personal Data has the meaning given to it in the Data Protection Legislation. Where such term is not defined by the Data Protection Legislation, it shall mean any information relating to, or directly or indirectly identifying a Data Subject.

Personal Data Breach has the meaning given to it in the Data Protection Legislation. Where such term is not defined by the Data Protection Legislation, it shall mean any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Processing has the meaning given to it in the Data Protection Legislation. Where such term is not defined by the Data Protection Legislation, it shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as (without limitation) collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and **Process** and **Processed** shall have corresponding meanings;

Subcontractor means any Third Party from time to time providing goods and/or services in connection with: (a) the provision of Products, Services and/or Deliverables; and/or (b) Processing or other use of any Protected Personal Data as permitted by a Contract.

Supplier/Third Party Personnel means any and all persons and/or entities that perform any part of the Services or provide any Product(s) under any Contract, including employees, Subcontractors, and/or agents of Supplier or any of its Subcontractors.

Supplier/ Third Party Systems means any electronic information systems (which may include one or more of hardware, equipment, software, peripherals and communications networks) which (or a part of which) are: (i) used to provide any Products or Services to any Barclays Affiliate in connection with a Contract, or (ii) maintained, administered, monitored or under the control of Supplier or a Subcontractor in connection with a Contract.

System means any electronic information system (which may include one or more of hardware, equipment, software, peripherals, and communications networks) which (or a part of which) are used to provide any goods or Services to any Barclays Affiliate in connection with a Contract.