BARCLAYS

External Supplier Control Obligations

Information and Cyber Security

For Suppliers Categorised as Low Information and Cyber Risk

Version 9.0 Dated April 2019

Control Title	Control Description	Why this is important
1. Information/Cyber Security Governance, Policy and Standards	The Supplier must have Information / Cyber risk governance processes in place that ensure an understanding of their technology environment and the state of Information and Cyber security controls, and a security program to protect the Supplier from Cyber threats in accordance with Good Industry Practice (including NIST, SANS, ISO27001) and applicable industry requirements. The Supplier shall undertake regular risk assessments in relation to Information/Cyber security and shall implement such controls and take such steps as are required to mitigate the risks identified. The Supplier must maintain senior management-approved policies, and standards to manage Supplier's Information/Cyber risk. The Supplier must define roles and responsibilities for Information/Cyber Security.	If this control is not implemented, Barclays or its Suppliers may not have and be able to demonstrate appropriate oversight on information/cyber security. Documented policies and standards are crucial elements for risk management and governance. They set the management's view of the controls required to manage Information/cyber risk.
2. Incident Management Process	Incident response process for timely handling and regular reporting of incidents involving Barclays Information and/or Services used by Barclays must be established and managed. The following must be defined as part of the incident response procedure: • Security incidents and data breaches that have affected or targeted Barclays assets and /or Services being provided to Barclays must be reported to Barclays as soon as possible and progress updates provided on remedial actions. • The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and informed to Barclays.	An incident management and response process helps to ensure that incidents are quickly contained and prevented from escalating.
3. Endpoint Security	The Supplier must ensure that endpoints used to access the Barclays network, or process Barclays Data, must be hardened to protect against attacks. This includes, but is not limited to, limiting attack surface through disabling of un-needed software/services/ports, ensuring all deployed versions are within public support periods,	If this control is not implemented, Barclays and Supplier network and endpoints may be vulnerable to cyber-attacks.

	malware protection and host firewall capabilities are in place and appropriately configured, and controls in place to mitigate exploitation attempts.	
4. Cloud Computing	All use of cloud computing (public/private/community/hybrid) service. SaaS/PaaS/IaaS used as part of the delivering services to Barclays must be adequately protected. Controls to protect Barclays Information and the service must be commensurate with the risk profile and criticality of the Information Asset to prevent data leakage and cyber breaches.	If this principle is not implemented, inappropriately protected Barclays Information Assets could be compromised, which may result in 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.	Anti-malware solutions are vital for the protection of Barclays Information assets against malicious code.
6. Network Security	The Supplier must ensure that all IT Systems operated by the Supplier or its sub-contractor which support services provided to Barclays are protected from lateral movement of threats within the Supplier's (and any relevant sub-contractors') network. The following protection mechanisms should be considered by the Supplier based on their service(s) provided to Barclays: **External connections:** 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. **Wireless access:** All wireless access to the network must be subject to authorisation, authentication, segregation and encryption protocols to prevent security breaches. **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). **Distributed Denial of Service (DDoS):** A defence in depth approach must be implemented in the network and key systems to protect at all times against service interruption via Cyber Attacks.	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.

	N.B. The term "network" as used in this control refers to any non-Barclays network for which the supplier is responsible for, including the Supplier's sub-contractor's network.	
7. Application Protection	The Supplier software / applications development ensure that all the key security activities have been incorporated into the software development process to prevent service interruptions, security vulnerabilities and Cyber Security breaches. 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. The Supplier must ensure that source code should be securely executed, stored and sent to Barclays.	Controls protecting application development help ensure that applications are secured at deployment.
8. Threat Simulation/ Penetration Testing/ IT Security Assessment	The Supplier must engage with an independent qualified security provider to perform an IT security assessment/penetration testing covering IT infrastructure and applications related to the service(s) that the Supplier provides to Barclays. This must be undertaken at least annually to identify vulnerabilities that could be exploited to breach the confidentiality of Barclays Data through cyber-attacks. The Supplier must operate a consistent mechanism for recording, triaging, and responding to identified vulnerabilities.	If this control is not implemented, Suppliers may be unable to assess the Cyber threats they face and the appropriateness and strength of their defenses.
9. Asset and Security Protection Technologies	Appropriate technologies must be applied to address current and emerging cyber threats with a consistent baseline of controls maintained to prevent attack delivery, execution, exploitation, and exfiltration. Host systems and network devices forming part of the Supplier Systems must be configured to function in accordance with Good Industry Practice (e.g. NIST, SANS, ISO27001). The assets or systems storing or processing it must be protected against physical tampering, loss, damage or seizure and inappropriate configuration or changes. Barclays' Information Assets stored in either physical or electronic form, when being destroyed or deleted must be performed in a secure way appropriate to its associated risk, ensuring that it is not recoverable. Systems must be configured securely to prevent unnecessary breaches. Monitoring and auditing and logging of systems must be in place to detect inappropriate or malicious activity.	If this control is not implemented, Barclays assets or assets used by Suppliers to service Barclays could be compromised, which may result in financial losses, loss of data, reputational damage and regulatory censure.

10. Logical Access Management (LAM)	Access to Information must be restricted, and with due consideration of the need-to-know, the Least Privilege and the segregation of duties principles. The Information Asset Owner is accountable for deciding who needs what access. • The need-to-know principle is that people should only have access to Information which they need to know in order to perform their authorised duties. For example, if an employee deals exclusively with UK-based customers, they do not "need to know" Information pertaining to customers based in the US. • The Least Privilege principle is that people should only have the minimum level of privilege necessary in order to perform their authorised duties. For example, if an employee needs to see a customer's address but will not be required to change it, then the "Least Privilege" they require is read-only access, which they should be given rather than read/write access. • The segregation of duties principle is that at least two individuals are responsible for the separate parts of any task in order to prevent error and fraud. For example, an employee who requests an account creation should not be the one who approves the request. These principles should be applied on a risk basis, taking into account the confidentiality rating of the Information. Each account must be associated with a single individual, who shall be accountable for any activity carried out using the account. This does not preclude the use of Shared Accounts, but a single individual must still be accountable for each Shared Account. Access management processes shall be defined as per Good Industry Practice and include the following as a minimum: • robust authorisation process in place prior to creating/amending/deleting accounts; • periodic User access review process; • mover controls – Access amended/removed within 5 working days of the move date; • leaver controls – All logical access used to provide services to Barclays removed within 24 hours of leave date, all other secondary access removed within 7 days; and • dormant accounts not used for 60 or more consecutive days must be suspended. • Passwords for interactive accounts must be changed at least every 90 days and must be different from the previous twelve (12) passwords. • Privileged Accounts must be changed after each use, and every 90 days minimum.	Appropriate LAM controls helps to ensure that Information Assets are protected from inappropriate usage.

	• Interactive accounts must be disabled after a maximum of five (5) consecutive failed attempts. Where remote access to Barclays Information Assets stored within supplier managed environment is allowed, two factor authentication and authorisation of the end point must take place taking into account the identity of the User, the type of device and the security posture of the device (e.g. patch level, status of anti-malware, rooted or not rooted mobile device, etc.).	
11. Data Leakage Prevention	The data leakage risk of Information related to the service(s) which the Supplier provides to Barclays egress through the network or physical medium must be assessed and mitigated. The following data leakage channels must be considered: • Unauthorised transfer of information outside the internal network/ supplier network. • Loss or theft of Barclays Information Assets on portable electronic media (including electronic information on laptops, mobile devices, and portable media); • Insecure information exchange with third parties; and • Inappropriate printing or copying of information	Appropriate data leakage prevention controls are a vital element of information security, helping ensure that Barclays Information are not lost.
12. Information Labelling Schema	***Where appropriate****, the Supplier must apply the Barclays Information Labelling Schema and handling requirements (Appendix B, Table B1 and B2), or an alternative scheme that is agreed with Barclays, to all Information Assets held or processed on behalf of Barclays. * "***where appropriate***" *refers to the benefit of labelling balanced against the associated cost. For example, it would be inappropriate to label a document if doing so would breach regulatory anti-tampering requirements.*	A complete and accurate inventory of Information assets is essential for ensuring appropriate controls.
13. Right of Inspection	The Supplier shall allow Barclays, upon Barclays giving not less than ten Business Days written notice, to conduct a security review of any site or technology used by the Supplier or its Sub-contractors to develop, test, enhance, maintain or operate the Supplier Systems used in the Services in order to review the Supplier's compliance with its obligations. The Supplier shall also allow Barclays to carry out an inspection immediately after a security incident. Any non-compliance of controls identified by Barclays during an inspection shall be risk assessed by Barclays and Barclays shall specify a remediation timeframe. The Supplier shall then complete any required remediation within that timeframe. The Supplier shall provide all assistance reasonably requested by Barclays in relation to any inspection.	If not agreed, Suppliers will be unable to provide full assurance of compliance to these security obligations.

Appendix A: Glossary

Definition	
Account	A set of credentials (for example, a user ID and password) through which access to an IT system is managed using logical access controls.
Advanced Persistent Threats (APT)	An advanced persistent threat (APT) is a stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period.
Denial of Service (Attack)	An attempt to make a computer resource unavailable to its intended users.
Destruction / Deletion	The act of overwriting, erasing or physically destroying information such that it cannot be recovered.
Information Asset	Any information that has value, considered in terms of its confidentiality, integrity, and availability requirements. Any singular piece or grouping of Information that has a value for the organisation. Typically grouped at a high (business process) level.
Least Privilege	The minimum level of access/permissions which enables a User or account to perform their business role.
Malicious Code	Software written with the intent to circumvent the security policy of an IT system, device or application. Examples are computer viruses, trojans and worms.
Multi-Factor Authentication	Authentication using two or more different authentication techniques. One example is the use of a security token, where successful authentication relies upon something that the individual holds (i.e. the security token) and something the user knows (i.e. the security token PIN).
Privileged Account	An account that provides an elevated level of control over a specific IT system. These accounts are typically used for system maintenance, security administration or configuration changes to an IT system. Examples include 'Administrator', 'root', Unix accounts with uid=0, Support Accounts, Security Administration Accounts, System Administration Accounts and local administrator accounts
Shared Account	An account granted to more than one employee, consultant, contractor or agency worker who has authorised access but individual accounts are not an option provided due to the nature of the system accessed.
System	A system, in the context of this document, is people, procedures, IT equipment and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.
User	An account appointed to a Supplier employee, consultant, contractor or agency worker who has authorised access to a system without elevated privileges.

Appendix B: Barclays Information Labelling Schema

Table B1: 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 • 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. • Audit findings and reports.
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.	• 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).

	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.	• Final research documents. • Non- Barclays Material Non-Public Information (MNPI). • All research reports • Certain marketing materials. • Market commentary.
Unrestricted	Information either intended for general distribution, or which would not have any impact on the organisation if it were to be distributed.	• Marketing materials. • Publications. • Public announcements. • Job advertisements. • Information with no impact to Barclays.

Table B2: Barclays Information Labelling Schema – 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	Restricted – Internal	Restricted – External	Secret
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 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.	• 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).
Access & Use	• 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.	• 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
Share	• 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 Suppliers 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 Suppliers 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.	• 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 Suppliers 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 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.	• Assets must not be faxed. • 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.
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	• 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. • Media on which Secret electronic assets have been stored must be appropriately sanitised prior to, or during, disposal.

Banking Secrecy

Additional controls only for Banking Secrecy Jurisdictions (Switzerland/Monaco)

Control Area / Title	Control Description	Why this is important
1. Roles and Responsibilities	The Supplier must define and communicate roles and responsibilities for the handling of Client Identifying Data (hereafter CID). The supplier must review documents highlighting roles and responsibilities for CID after any material change to the Supplier's operating model (or business) or at least once a year and distribute them with the appropriate banking secrecy jurisdiction Key roles must include a senior executive, accountable for the protection and oversight of all activities related to CID (Please refer to Appendix A for the definition of CID)	Clear definition of roles and responsibilities supports the implementation of the External Supplier Control Obligations Schedule.
2. CID Breach Reporting	Documented controls and processes must be in place to ensure any breaches that impact CIDs are reported and managed. Any breach of the handling requirements (as defined in table C2) must be responded to by the Supplier and reported to the corresponding banking secrecy jurisdiction immediately (at the latest within 24 hours). An incident response process for timely handling and regular reporting of events involving CID must be established. The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and shared and agreed with the corresponding banking secrecy jurisdiction .	An incident response process helps to ensure that incidents are quickly contained and prevented from escalating. Any breach that impact CID could have strong reputational, damage to Barclays and could lead to fines and loss of the banking licence in Switzerland or Monaco
3. Education and awareness	Supplier employees that do have access to CIDs and/or handle them must complete a training* which implements the CID Banking Secrecy Requirements after any new change in regulations or at least once a year. The Supplier must ensure that all new supplier employees (that have access to CIDs and/or handle them), within reasonable time period (circa 3 months), complete training which ensures they understand their responsibilities with regards to CID. Supplier must keep track of employees that completed training. * banking secrecy jurisdictions to provide guidance on the training expected content.	Education and awareness supports all other controls within this schedule.

4. Information Labelling Schema	***Where appropriate****, the Supplier must apply the Barclays Information Labelling Schema (Table C1 of Appendix C), or an alternative scheme that is agreed with the banking secrecy jurisdiction, to all Information Assets held or processed on behalf of the banking secrecy jurisdiction. The handling requirements for CID data are provided in Table C2 of Appendix C. * "***where appropriate***" *refers to the benefit of labelling balanced against the associated cost. For example, it would be inappropriate to label a document if doing so would breach regulatory anti-tampering requirements.*	A complete and accurate inventory of Information assets is essential for ensuring appropriate controls.
5. Cloud Computing/External Storage	All use of cloud computing and/or external storage of CID (in servers out the banking secrecy jurisdiction or out of the Supplier infrastructure) used as part of the service to that jurisdiction must be approved by corresponding relevant local teams (including Chief Security Office, Compliance and Legal); and controls must be implemented in accordance with the corresponding banking secrecy jurisdiction to protect inadequacy CID information with regards to the high risk profile they present.	If this principle is not implemented inappropriately protected Customer data (CID) could be compromised, which may result in legal and regulatory sanction, or reputational damage.

** Client Identifying data are special data due to the Banking Secrecy laws in vigour in Switzerland and Monaco. As such, the controls listed here are complement to those listed above.

Term	Definition
CID	Client Identifying Data,
CIS	Cyber And Information Security
Supplier employee	Any individual directly assigned to the supplier as permanent employee, or any individual providing services to the supplier on a limited period of time (such as a consultant)
Asset	Any singular piece or grouping of information that has a value for the organisation
System	A system, in the context of this document, is people, procedures, IT equipment and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.

User	An account appointed to a Supplier employee, consultant, contractor or agency worker who has authorised access to a Barclays owned system without elevated privileges.

Appendix B: CLIENT IDENTIFYING DATA DEFINITION

Direct CID (DCID) can be defined as unique identifiers (owned by the client), which allow, as is and by itself, to identify a client without access to data in Barclays banking applications. This must be unambiguous, not subject to interpretation, and can include such information as first name, last name, company name, signature, social network ID etc. Direct CID refers to client data that is not owned or created by the bank.

Indirect CID (ICID) is split up into 3 levels

- **L1 ICID** can be defined as unique identifiers (owned by the Bank) which allow to uniquely identify a client in the case access to banking applications or other **third party applications** is provided. The identifier must be unambiguous, not subject to interpretation, and can include identifiers such as the account number, the IBAN code, credit card number, etc.

- **L2 ICID** can be defined as information (owned by the client) which, in combination with another, would provide inference to the identity of a client. While this information cannot be used to identify a client on its own, it can be used with other information to identify a client. L2 ICID must be protected and managed with the same rigor as DCID.

- **L3 ICID** can be defined as unique but anonymised identifiers (owned by the Bank) which allow to identify a client if access to banking applications is provided. The difference with L1 ICID is the Information Classification as Restricted - External instead of banking secrecy, meaning they are not subject to the same controls.

Please refer to Figure 1 CID Decision Tree for an overview of the classification method.

Direct and Indirect L1 ICID must not be shared with any person located outside of the Bank and must respect the need-to-know principle at any time. L2 ICID can be shared on a need-to-know basis, but must not be shared in conjunction with any other piece of CID. By sharing multiple pieces of CID there is a possibility of creating a 'toxic combination' which could potentially reveal the identity of a client. We define a toxic combination starting from at least two L2 ICID. L3 ICID can be shared as they are not classified as Banking Secrecy level information, unless recurrent usage of the same identifier can result in the gathering of sufficient L2 ICID data to reveal the identity of the client.

Information Classification	Banking Secrecy			Restricted - Internal
Classification	**Direct CID (DCID)**	**Indirect CID (ICID)**		
		Indirect (L1)	**Potentially Indirect (L2)**	**Impersonal Identifier (L3)**
Type of Information	Client name	Container number / Container ID	First name	Internal processing ID
	Company name	MACC (money account under an Avaloq Container ID) number	Date of birth	Static unique identifier
	Account statement	Address	Nationality	Dynamic identifier
	Signature	IBAN	Title	External container ID
	Social network ID	eBanking logon details	Family situation	
	Passport number	Safe deposit number	Post code	
	Phone number	Credit card number	Wealth situation	
	Email address		Last Name	
	Job title or PEP title		Last Customer Visit	
	Artist Name		Language	
	IP Address		Gender	
	Fax number		CC Expiration Date	
			Primary Contact Person	
			Place of Birth	
			Account Opening Date	

			Large Position/Transaction Value	

Example: If you send an email or share any document with external people (included third parties in Switzerland/Monaco) or internal colleagues in another affiliate/subsidiary located in Switzerland/Monaco or other countries (e.g. UK)

1. Client name

   (DCID) = Banking Secrecy Breach

2. Container ID

   (L1 ICID) = Banking Secrecy Breach

3. Wealth situation + Nationality

   (L2 ICID) + (L2 ICID) = Banking Secrecy Breach

Appendix C: Barclays Information Labelling Schema

Table C1: Barclays Information Labelling Schema

** The Banking Secrecy label is specific to Banking Secrecy jurisdictions.

Label	Definition	Examples
Banking Secrecy	Information which is related to any Swiss, Direct or Indirect Client Identifying Data (CID). The 'Banking Secrecy" classification applies to information which is related to any Direct or Indirect Client Identifying Data. Therefore, access by all employees, even located in the owning jurisdiction is not appropriate. Access to this information is only required by those with a need-to-know to fulfil their official duties or contractual responsibilities. None authorised disclosure, access or sharing both internally and externally of the entity of such information may have a critical impact and may lead to criminal proceedings and have civil and administrative consequences such as fines and loss of the banking licence, if it were disclosed to unauthorised personnel both internally and externally.	• Client name • Client address • Signature • Client's IP address (further examples in Appendix B)

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).	• Strategies and budgets. • Performance appraisals. • Staff remuneration and personal data. • Vulnerability assessments. • Audit findings and reports.

	This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	
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.
Unrestricted	Information either intended for general distribution, or which would not have any impact on the organisation if it were to be distributed.	• Marketing materials. • Publications. • Public announcements. • Job advertisements. • Information with no impact to Barclays.

Table C2: Information Labelling Schema – Handling Requirements

** Specific handling requirements for CID data to ensure their confidentiality as per regulatory requirements

Lifecycle Stage	Banking Secrecy requirements
Creation and Labelling	As per "Restricted-External" and: • Assets must be assigned an CID Owner.
Store	As per "Restricted-External" and: • Assets must only be stored on removable media for as long as explicitly required by a specific business need, regulators or external auditors. • Large Volumes of Banking Secrecy Information Assets must not be stored on portable devices/media. For more information, contact local Cyber and Information Security Team (hereafter CIS). • Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them, according to the need-to-know or need-to have principle. • Secure workplace practices such as Clear Desk and Desktop locking must be followed for safekeeping of assets (whether physical or electronic). • Removable media information assets must only be used for storage for as long as it is explicitly required, and locked away when not in use. • Ad-hoc data transfers to portable devices/ media requires the data owner, compliance and CIS approval.
Access & Use	As per "Restricted-External" and: • Assets must not be removed / viewed off site (Barclays premises) without formal authorisation from the CID Owner (or deputy). • Assets must not be removed / viewed out of the client booking jurisdiction without formal authorisation from the CID Owner(or deputy) and the client (waiver/ Limited Power of Attorney). • Secure remote working practices, ensuring no Shoulder Surfing is possible, must be followed when taking physical assets off site.
	• Ensure that unauthorised persons cannot observe or access the electronic assets containing CID through the use of restricted access to business applications.
Share	As per "Restricted-External" and: • Assets must only be distributed in accordance with the "need to know principle" AND within the originating Banking Secrecy jurisdiction's information systems and staff. • Assets being transferred on an ad-hoc basis using removable media requires the information asset owner and CIS approval. • Electronic Communications must be encrypted while in transit.

	• Assets (hard copy) sent by mail must be delivered using a service that requires a confirmation receipt. • Assets must only be distributed in accordance with the "need to know principle".
Archive and Dispose	As per "Restricted-External"

*** 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	Restricted – Internal	Restricted – External	Secret
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 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.	• 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).
Access & Use	• 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.	• 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	• 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).

	• Electronic assets must be protected by appropriate Logical Access Management controls if required	not possible, secure printing tools must be used. • Electronic assets must be protected by appropriate Logical Access Management controls.	• Printed assets must be printed using secure printing tools. • Electronic assets must be protected by appropriate Logical Access Management controls
Share	• 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 Suppliers 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 Suppliers 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.	• 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 Suppliers 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. • 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.

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	• 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. • Media on which Secret electronic assets have been stored must be appropriately sanitised prior to, or during, disposal.