GROUP PHYSICAL & PEOPLE SECURITY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

LLOYDS BANKING GROUP	**PHYSICAL & PEOPLE SECURITY POLICY** **SUMMARY FOR THIRD PARTY SUPPLIERS**

RATIONALE

Group Policy Rationale

This Policy has been designed to assist in managing the physical and people security risks to protect our people, customers, branches, buildings and company assets. The overall risk includes the failure to:

- Identify and report risks and threat to the safety of colleagues (during the course of business activities), customers, branches, buildings and assets.
- Gather and assess security threat monitoring intelligence.
- Properly conduct and refresh Business Unit Risk Assessments (including risks assessments in the branch network) to highlight key activities.
- Assess the risk ratings of group buildings and undertake building risk assessments in line with the agreed schedule and standards.
- Assess the impact of changes to new / existing buildings including refurbishments.
- Implement findings of branch, Business Unit and building risks assessments in line with risk appetite
- Act / communicate upon security threat monitoring intelligence.
- Provide the adequate level of surveillance and monitoring over group buildings.
- Prevent unauthorised access to Group sites.
- Deliver required level of colleague protection.
- Respond to an incident and investigate root cause to identify key outcomes and learnings.

Through this approach, the Group will maintain customer confidence, protect the Group's customers, colleagues, commercial interests and reputation.

A physical security incident is defined as *any attempted or committed criminal, extremist, malicious or terrorist act; or suspicion thereof*.

In addition, this Policy has been designed to support compliance with the following legislation and / or regulations:

- The physical security requirements recommended in FCA Financial Crime: A Guide for Firms (Parts 1 & 2).
- Provision of security in line with the Payment Card Industry – Department for Security Standards requirements (Requirement 9). Restrict physical access to cardholder data.
- Recommendations for security provision as provided by Joint Terrorism Analysis Centre (JTAC) and the Centre for the Protection of the National Infrastructure (CPNI)
- Data Protection Act 2018

- General Data Protection Regulation (EU) 2016/679

Customer Impact.

The Group's vision is to be the best bank for customers. The Physical & People Security Policy supports this vision by providing a safe and secure environment for our customers and their assets.

SCOPE

This third party version of the Policy applies to suppliers where it has been identified that the Group Policy applies to the provision of their goods and or services.

. In particular any who are responsible for:

- Any of the Group's customer, employee or financial information,
- Material assets or property belonging to the Group; and / or
- The safety of Group personnel or those of suppliers acting on behalf of Lloyds Banking Group.

MANDATORY REQUIREMENTS – GENERAL

All Suppliers in scope of this Policy must:

- Appoint an individual to be responsible for physical security;
- Conduct a review of physical security environment and physical security risks at least annually or whenever there is a significant risk to the Group's material information, assets or property;
- Have an appropriate and auditable access control mechanism in place to ensure only authorised personnel are permitted to enter the supplier's premises, the logs must be retained for 12 months
- Have robust processes in place to ensure all visitors to their premises are logged and supervised. The logs must be retained for 12 months;
- Ensure their premises are equipped with an appropriate CCTV system to monitor and premises entry / exit points and secure areas.
- Recorded CCTV images must be securely stored for a minimum of 30 days or where data is stored or is governed by specific regulations such as PCI-DSS, this retention period should be 90 days;
- Ensure their premises are equipped with an appropriate intrusion detection system. This must be monitored 24/7;
- Ensure that all electronic security systems are installed and maintained by a contractor who is approved by a recognised authority.

Training

Suppliers must provide physical & people security training and awareness as a part of their employee induction process and ensure it is repeated annually by all employees.

Incident Reporting

The Supplier must include in their Security Policy a procedure ("**Security Incident Management Procedure**") for reporting all physical security incidents.

The Security Incident Management Procedure must detail the following obligations of

the Supplier, all of which must be invoked as soon as reasonably possible upon becoming aware of a Security Incident, and in any event within 24 hours of the occurrence of the Security

Incident.

Security Audits

Lloyds Banking Group reserves the right to undertake assurance of the security arrangements and processes relating to the Supplier's and/or its Approved Subcontractors' provision of the Services once in each 12 month period during the Term of the Agreement and additionally following a security event.

Risks or control weaknesses identified from Lloyds Banking Group security assurance work must be addressed and / or rectified within timescales agreed by Chief Security Office.

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Supplier to report to the Supplier Manager and/or relevant Group contact any security events which impact the Group	100% of incidents are reported within 24hrs	Following any event that impacts the Group
Supplier to make available MI on the completion of physical & people security training completed by all employees	• % of employees completed annual training • % of new starts completed training within 8 weeks of commencing employment with the supplier	Annually

MANDATORY REQUIREMENTS – NON-COMPLIANCE

Any material differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager.

The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward.

Version Number	Effective Date
1.0 Approved	April 2014
2.0 Approved	April 2015

3.0 Approved	April 2016
4.0 Approved	May 2017
5.0 Approved	July 2018
Next Planned Revision: July 2019	