PHYSICAL SECURITY POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 4

1.1. Document Definition 4

1.2. Objective 4

1.3. Scope 4

Applicability to employee 4

1.1.1 Applicability to External Parties 4

1.1.2 Applicability to Assets 4

1.4. Related Documents / References 5

2. Policy Statements 6

1.5. Physical Security Facility Approval and Plan 6

FACILITY ACCESS 6

1.6. Working in Restricted Area Procedures 6

1.7. Physical Access to Sensitive Information 6

1.8. Access to Computer and Communications Assets 6

1.9. Unauthorised Physical Access Attempts 6

1.10. Access Control System Records 7

1.11. Access to Restricted Areas - Post Termination 7

1.12. Physical Access Monitoring 7

1.13. Access Monitoring Tamper Resistance 7

1.14. Physical Access Badge Procedures 7

1.15. Physical Access Badge System Access 7

1.16. Identification Badges 7

1.17. Temporary Badges 7

1.18. Badge-Controlled Access 8

1.19. Access ‘Piggy-Backing’ 8

1.20. Individuals Without Identification Badges 8

1.21. Visitor Identification 8

1.22. Third-Party & Visitor Access 8

1.23. Visitor Badge - Identification 8

1.24. Visitor Badge - Expiration 8

1.25. Visitor Badge - Surrender 8

1.26. Visitor Log - Contents 8

1.27. Visitor Log - Retention 9

1.28. Physical Security Plan Review 9

1.29. Restricted Area Access List(s) 9

1.30. Access Monitoring Reviews 9

1.31. Testing of Physical Security Perimeter 9

EQUIPMENT PROTECTION & ENVIROMENTAL CONTROLS 9

1.32. Asset Location & Protection 9

1.33. Protection of Portable Devices 9

1.34. Protection of Off-Premise Assets 9

1.35. Preventative Maintenance 10

1.36. Secure Facility Design 10

1.37. Critical Cabling Design 10

1.38. Environmental Controls 10

1.39. Supporting Utilities 10

1.40. Removal of Assets 11

1.41. Treatment of Removed Assets 11

DATA PROTECTION 11

1.42. Clear Screen 11

1.43. Clear Desk 11

3. Policy Compliance & Enforcement 13

1.45. Compliance Measures 13

1.46. Enforcement 14

4. Exception Process / Glossary 15

1.47. Exception Process 15

1.48. Glossary / Acronyms 15

5. Document Management 16

5.1 Document Revision Log 16

5.2 Document Ownership 17

5.3 Document Coordinator 17

5.4 Document Approvers 17

5.5 Document Distribution 17

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see *ZBL-POL-ALL-001 - Information Security Policy Framework*.

## Objective

Zenith Bank UK will ensure, so far, as is reasonably practicable, that employees, and other non-employees are protected from risks to their health, safety and welfare.

Measures will be adopted to aid the safety and security of staff, visitors and unauthorised visitors to the Zenith Bank as well as helping to reduce the potential for arson, theft and vandalism. Building security procedures will include arrangements to ensure, as far as is reasonably practicable, that unauthorised visitors are prevented from entering the Zenith Bank premises and that, should these systems fail, procedures are in place to deal with unauthorised visitors should they gain access. Furthermore, Zenith Bank will review security controls to prevent a reoccurrence of any unauthorised entry.

Management responsibility for the Zenith Bank’s security is shared between the Zenith Bank and Facilities Group.

The objective of this policy is to provide information security requirements to restrict physical access to areas housing information systems to authorised individuals, as well as protect those areas from environmental hazards.

## Scope

### Applicability to employee

XXXX refers to XXXX. as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *ZBL-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-005 - Data Handling & Retention Policy*
* *XXXX-POL-ALL-022 - Telecommuting & Mobile Computing Policy*
* *XXXX-STD-ALL-023 - Physical Security Standards*

# Policy Statements

## Physical Security Facility Approval and Plan

All information processing facilities must be approved and authorised by the SC. All facilities must undergo a risk assessment and each facility must meet the bank’s requirements. Any deviation or non-compliance issue resulting from this review must be addressed and resolved within an appropriate amount of time as determined by the SC.

Every XXXX facility must have a physical security plan, with plan accountability formally assigned to a senior manager in charge of the facility.

Plan must cover the defined security perimeters of facilities that contain critical or sensitive information assets.

## FACILITY ACCESS

## Working in Restricted Area Procedures

Procedures for working in restricted areas at all XXXX locations must be developed, documented, distributed and be accompanied by appropriate training and enforcement controls. Restricted access areas are those that pose a high risk which may be areas that house secure and/or confidential records, i.e. communications rooms.

## Physical Access to Sensitive Information

Access to every office, computer room, and work area containing sensitive information must be physically restricted to limit access to those with a job-related need. This will be enforced with educating employees on the best network security practices including password protection, in-line with a robust policy handling sensitive data as detailed in the *XXXX-POL-ALL-005 - Data Handling & Retention Policy and XXXX-POL-ALL-015 - Security Awareness & Training Policy*

## Access to Computer and Communications Assets

Facilities that house XXXX computers or communications assets must be protected with physical security measures that prevent unauthorised persons from gaining access.

## Unauthorised Physical Access Attempts

employees must not attempt to enter restricted areas in XXXX buildings for which they have not received explicit authorisation.

## Access Control System Records

The Landlord / Facilities Management must maintain records of the persons currently and previously inside XXXX facilities and securely retain this information for at least one year.

## Access to Restricted Areas - Post Termination

Terminated employees must all have access rights to XXXX restricted areas immediately revoked.

## Physical Access Monitoring

Method - Video cameras or other access control mechanisms that monitor an individual’s entry and exit to restricted areas must be in place. The use of Manned, Physical and Technical security methods must be in place to achieve this

## Access Monitoring Tamper Resistance

Security - Video cameras or other access control mechanisms that monitor restricted areas must be protected from tampering and disabling.

Access points to restricted areas (delivery and loading areas etc.) must be controlled and, if possible, isolated from restricted processing facilities.

## Physical Access Badge Procedures

Procedures must be developed and implemented that control the issuance, modification, and revocation of XXXX physical access badges.

## Physical Access Badge System Access

Access to the system that controls the XXXX physical access badges must be limited to only those employees with the responsibility to issue, modify, or revoke physical access badges.

## Identification Badges

When in a XXXX restricted building or facility, all persons (employees, contractors and visitors) must wear an identification badge that is clearly visible.

## Temporary Badges

Workers who have forgotten their identification badge must obtain a temporary badge by providing an appropriate identification.

## Badge-Controlled Access

Each employee must present their badge to the badge reader before entering every controlled door within XXXX facilities.

## Access ‘Piggy-Backing’

Workers must not permit known, unknown or unauthorised persons to pass through doors, gates, and other entrances to restricted areas without requesting a positive swipe of the person’s badge.

## Individuals Without Identification Badges

Individuals without a proper XXXX identification badge in a clearly visible place must be immediately questioned about their badge and if they cannot promptly produce a valid badge, they must be escorted to the receptionist desk.

## Visitor Identification

All visitors to XXXX must show picture identification and sign a log prior to gaining access to restricted areas.

## Third-Party & Visitor Access

Visitors or other third-parties accessing XXXX offices, computer facilities, and other work areas containing sensitive information must be escorted at all times by qualified personnel.

## Visitor Badge - Identification

All visitors must be provided with a badge or other artefact that clearly identifies them as a non-employee.

## Visitor Badge - Expiration

All visitor artefacts must be set to expire in line with their approved period of stay on the premises or provide no access to any part of the facility.

## Visitor Badge - Surrender

All visitors must surrender their artefact to the issuing party or their employee escort before leaving any XXXX facility.

## Visitor Log - Contents

A visitor log must be maintained that contains the visitor's name, the firm represented, and the employee authorising physical access to any XXXX facility.

## Visitor Log - Retention

Visitor logs must be retained for at least a year.

## Physical Security Plan Review

The physical security plan for each facility must be reviewed annually and acceptance by the accountable senior manager formally recorded.

## Restricted Area Access List(s)

A complete list of all employees with access to restricted areas must be maintained, reviewed, and updated annually by the responsible Head of Department

## Access Monitoring Reviews

Video camera or other access control mechanism output that monitor the entry and exit points to secure areas must be monitored daily.

## Testing of Physical Security Perimeter

XXXX will perform a comprehensive testing of the physical security controls of each location at least annually. This testing includes at the minimum physical access controls, physical access monitoring controls and logging controls.

## EQUIPMENT PROTECTION & ENVIROMENTAL CONTROLS

## Asset Location & Protection

All ‘core processing’ assets, including, but not limited to; network devices, telecoms systems, and business-critical servers must be located within a secure data centre or suitably secured area.

## Protection of Portable Devices

Easily portable computers and components (e.g. laptop computers, PDAs, wireless cards) must be physically secured to protect from theft or unauthorised access.

## Protection of Off-Premise Assets

The use of any information system asset outside the XXXX facilities must be authorised. This applies to equipment owned by the XXXX and that owned employee and used on behalf of XXXX.

The following rules apply:

* information system assets taken off-premises must not be left unattended in public places;
* vendor instructions for the protection of assets should be observed at all times;
* controls for off-premises locations, such as home-working, teleworking and temporary sites must follow the requirements as detailed in the *XXXX-POL-ALL-022 - Telecommuting & Mobile Computing Policy*, and;
* when off-premises assets are transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at a minimum the names and organisations of those who are responsible for the protection of the asset.

## Preventative Maintenance

Preventative maintenance must be performed on all information system assets in accordance with vendor recommended best practices and warranty requirements (if applicable).

All maintenance work must be performed by authorised and qualified personnel.

## Secure Facility Design

The design, installation and maintenance of secure facilities or areas must be performed by a formally qualified individual who follows current industry acceptable security standards and best practices.

## Critical Cabling Design

The design, installation and maintenance of critical cabling (e.g. power, telecoms etc.) must be performed by a formally qualified individual who follows current industry acceptable security standards and best practices.

## Environmental Controls

Data centre facilities or secure area management must provide and adequately maintain the following:

* fire detection and suppression, and;
* water / flood damage precautions;
* Physical security systems

## Supporting Utilities

Data centre facilities management must provide and adequately maintain the following:

* uninterruptable power supply;
* emergency lighting;
* HVAC, and;
* humidity control.

## Removal of Assets

Before any XXXX information system asset is sold, reused, destroyed donated, or otherwise removed from production, the written approval must first be provided by the [Executive Management].

## Treatment of Removed Assets

Prior to any form of disposal or reuse of a XXXX information system asset, all XXXX information must be securely removed.

Treatment must comply with the requirements are detailed in the *XXXX-POL-ALL-005 - Data Handling & Retention Policy* and *XXXX-POL-ALL-025 - Information Disposal Policy*

## DATA PROTECTION

## Clear Screen

All electronic systems (e.g., servers, workstations, desktops, and/or laptop computers) must clear the screen after a pre-defined period of time.

* Computers / computer terminals should not be left logged on when unattended and should be password protected.
* Computer screens should be angled away from the view of unauthorized persons.
* The screen is set to automatically lock when there is no activity for a period of ten (10) minutes for windows system and twenty (20) minutes for Unix system/servers.
* CTRL+ALT+DEL is used to lock computer screens when leaving computer systems.
* Users must "log off" their computers when their workspace is unattended.
* Users must "shut down" their computers at the end of the workday.
* Passwords must not be left on sticky notes posted on or under a computer, nor written down in an accessible location.
* Whiteboards containing Restricted and/or Sensitive information should be erased.
* Personal computers and computer terminals should be switched off when not in use and should be password protected.

## Clear Desk

Physical files, documents, hard copy materials, and removable storage media (e.g. CDs, diskettes, flash drives and external drives) containing must be physically secured to protect against theft or copying.

* All employees of Zenith bank UK are expected to tidy their desk of papers and any files in hardcopy or electronic form with personal/ confidential / sensitive information in them especially customer related records when leaving for the day / during short breaks.
* Each department shall provide a locker or filing cabinets for the purpose of complying with the clear desk policy. The desk locker or filing cabinets must be kept closed and locked when not in use or when not attended.
* Keys used for access to restricted or sensitive information must not be left at an unattended desk.
* Where applicable ensure any paper is shredded before being thrashed if it contains personal or confidential data.
* Employees where possible should not print off emails to read as this can result in information theft / leakage.
* Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
* Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday

# Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For a selection of networking, telecommunications, and server equipment, evidence that the equipment is stored in a secured facility. | * Facility documentation identifying the security controls utilised. * Observe equipment location |
| For a selection of IT facilities, evidence that they are protected from unauthorised access. | * Observe access to the selected facilities |
| For a selection of authorised facility access, evidence that it was approved by management. | * Copies of access approvals |
| For visitor access, evidence that the access was for an authorised purpose, recorded, supervised, and security information was provided. | * Copies of facility visitor logs * Observe visitor access procedures |
| For a selection of easily portable devices, evidence that they are protected from theft. | * For laptops, observe physical security * Inspect for unsecured portable components * For PDA’s please see the Mobile Computing Policy |
| For a selection of facilities or areas containing technology, evidence that documents and removable media such as laptops, flash media, and CD’s are protected from theft. | * Inspect selected areas for loose documentation and unsecured media |
| For a selection of facilities or areas and systems, evidence that the systems clear the screen after a pre defined period of time. | * Observe the screen clearing |
| For a selection of facilities or areas, evidence that controls are in place for the protection of documentation and media. | * Observe physical storage of documents and media * Inspect selected areas for loose documentation and unsecured media * Obtain copies of media transfer or disposal procedures |
| For a selection of facilities, evidence that they are protected from environmental hazards. | * Inspect facility for HVAC, Fire Suppression, Emergency Lighting, Power Protection, and Environmental Monitoring |
| For a selection of facilities, evidence that voice and data cables or lines are secured. | * Inspect voice and data cables for shielding, burial, conduit, or special routing |
| For a selection of access control devices, evidence that the data from these devices was recorded and stored. | * Logs recorded by devices * Video archive inventory lists * Screenshots of archived data (video files, card swipe logs, etc.) |
| For a selection of facilities, evidence that access was reviewed and revoked appropriately. | * Copies of access reviews * Documentation of access removal related to the reviews |
| For a selection of user’s evidence that clear screen and clear desk reviews were done | * Copies of review reports from internal audit/compliance |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *ZBL-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| HVAC | Heating Ventilation and Air Condition |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY

## Document Coordinator

This Policy is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff