PHYSICAL SECURITY STANDARD

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

INTERNAL Information

This document contains confidential information and is the property of XXXX. Distribution is restricted to XXXX and restricted third parties as approved by the document owner. By accepting this document, the recipient agrees not to provide this document or any information contained therein to any third party without express prior written consent of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Standard Statements 4

2.1 Secure Area Definition 4

2.2 Other Defined Areas 4

2.3 Security Control Requirements 4

2.4 Security Control Testing 4

2.5 Physical Entry Controls Review 4

3. Detailed Configuration Requirements 6

3.1 Access Control System Records 6

3.2 Physical Access Monitoring 6

3.3 Access Monitoring Tamper Resistance 6

3.4 Delivery and Loading Areas 6

3.5 Physical Access Badge Procedures 6

3.6 Other Measures 6

4. Standard Compliance & Enforcement 10

4.1 Compliance Measures 10

4.2 Enforcement 11

5. Exception Process / Glossary 12

5.1 Exception Process 12

5.2 Glossary / Acronyms 12

6. Document Management 13

6.1 Document Revision Log 13

6.2 Document Ownership 13

6.3 Document Coordinator 13

6.4 Document Approvers 13

6.5 Document Distribution 13

# Introduction

## Document Definition

This document is a Standard.

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

## Objective

The Physical Security Standard defines the detailed baselines to “good practice” that safeguard the XXXX’s physical assets.

The objective of this Standard 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 Employees

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

### Applicability to External Parties

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

### Applicability to Assets

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

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework - Information Security Policy Framework*
* *XXXX-POL-ALL-023 - Physical Security Policy*

# Standard Statements

## Secure Area Definition

‘Secure areas’ are those areas requiring a higher level of control. Currently, these are the areas deemed secure:

* Computer Rooms
* Dealing Rooms
* IT Office
* Human Resources Office

## Other Defined Areas

* Documents storage areas

## Security Control Requirements

All Secure Areas must include the following controls:

* Doors that automatically close after being opened;
* Secure Areas must not have windows that can be opened outside of an emergency scenario, and must be alarmed accordingly;
* Smoke, humidity, and temperature sensors linked to an incident response process;

## Security Control Testing

* Fire suppression and alarm systems must be tested on a semi-annual basis.
* Fire drill to be conducted on a semi-annual basis.

## Physical Entry Controls Review

Access rights to all areas must be reviewed at least on an annual basis.

Access to areas deemed 'secure areas' e.g. computer rooms and dealing rooms, must be reviewed at least annually

Only authorised employees are allowed access to areas deemed ‘secure areas’

Employees will only be given access to secure areas with the written approval of the Head of Department in charge of the secure area.

All employees are to use their access cards to enter the building and respective offices. The access card must also be used to gain access to a floor through the lift or stairs.

All employees are always to wear their XXXX red lanyards while in the office

# Detailed Configuration Requirements

## Access Control System Records

The (Landlord / Facilities Management) must maintain records of the persons currently and previously enrolled on the access control systems for XXXX facilities and securely retain this information for at least 1 (one) year on an offsite storage facility.

## Physical Access Monitoring

Video cameras, access cards or other access control mechanisms that monitor an individual’s entry and exit to XXXX facilities must be in place. The methods utilised include:

• Access Control, (Pedestrian);

• ID Passes that clearly show Zenith logo, level of clearance and Photo of Holder;

• Physical Security (Barriers, Fences, Locks etc.);

• CCTV;

• SIA licensed Manned Guarding;

## Access Monitoring Tamper Resistance

CCTV, access cards or other access control mechanisms that monitor XXXX facilities including restricted areas must be protected from tampering and disabling. This is undertaken through cameras being mounted high, keeping hidden and installed protective housing. XXXX will perform a comprehensive testing and review of the physical security controls of each location at least annually. This will include log reviews, archiving period, false positive rate and administrative user reviews.

## Delivery and Loading Areas

Anyone who delivers packages for XXXX should remain at the building’s reception, the front house employees/security are responsible for notifying the XXXX employee who expects the delivery. If an employee is unable to receive their order. Front house/security may accept the order on the employee’s behalf upon request.

## Physical Access Badge Procedures

Human Resources and Facilities management control the issuance, modification, and revocation of XXXX physical access badges as outlined in Human Resources policies and procedures

## Other Measures

* All employees of XXXX, contractors, consultants and other visitors shall be required to have the XXXX’s approved identification badges on when on the premises of the XXXX.
* Entrance into the XXXX’s premises shall be restricted through the use of locks, keys, biometric locks, security guards, walls, card-controlled entry or fingerprint recognition doors, manned reception desk and any other appropriate tools for restricting access.
* A security register shall be maintained at all the XXXX’s locations to access areas where equipment / devices supporting communication, data processing and storage are maintained.
* Physical access to the XXXX’s information systems facilities is to be restricted to authorized persons only. Authorization to enter restricted facilities is to be granted only when there is a business or technical reason for the person to enter the premises.
* Passes shall be zoned appropriately for secure areas (restricted zones) such as the IT Data Centre rooms as they require a higher level of security.
* Secure areas (restricted zones) must be protected with access control devices e.g. physical barriers, intrusion alarms, access-logging equipment such as card key systems and security cameras to ensure that only authorized personnel are allowed access.
* Access to sensitive or critical information processing facilities outside normal working hours must be specifically authorized and logged.
* Visitors are required to sign in to the visitors/contractors register at main reception.
* All visitors/contractors are to be given access cards permitting them to the floor for which they are visiting. One access card is issued per visitor/contractor
* If an unescorted person is seen around the office, staff are encouraged to politely challenge them.
* Under no circumstances, should a visitor be allowed to connect their own computer equipment to XXXX’s network, unless approved and authorized.
* Physical access rights must be revoked immediately upon termination/resignation of employees or completion of a consultation or vendor agreement.
* Data center, equipment rooms, and telecommunications closets must be protected from unauthorized or unnecessary access. The construction of data centers, equipment rooms, and telecommunication closets must take into account:
* Specifications developed as a response to potential threats to the asset.
* Specifications developed in accordance with the *XXXX-POL-ALL-004 -* XXXX Data Classification Policy.
* Vendor Specifications.
* All data centers, equipment rooms, and telecommunications closets must be locked when unattended.
* The office cleaners are an exception to the visitor rules set out above. They have been specifically vetted by the approved third party organization providing cleaning services to XXXX and as a result are the only visitors who are permitted to the non-restricted part of the office
* However, even in the case of the cleaners, extra vigilance should be applied with regard to information security. Sensitive information is placed in the locked cabinets during out-of-office hours. Employees are to ensure that all filing cabinets and sensitive areas are locked and the keys are stored in the appropriate location
* Environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities
* Hazardous or combustible materials should be stored at a safe distance from a secure area.
* Backup equipment and media should be sited at a safe distance to avoid damage from a disaster affecting the main site
* Appropriate firefighting equipment should be provided and suitably placed.
* All information assets should have adequate maintenance plans and/or insurance based on the value of the asset.
* Information assets must not be moved from its location unless authorized by the asset owner.
* Assets must be protected from power failures, electrical anomalies, fire, flood, an
* d other environmental hazards.
* Information assets must be protected from disruptions caused by failures in supporting utilities such as HVAC, water supply and sewage
* Critical Information assets must be supported by uninterruptible power supply (UPS). A backup power generating equipment should also be in place where possible.
* Power supply backup equipment including UPS’s, backup generators etc. must be subject to regular maintenance and testing.
* Power and telecommunications cables carrying data or supporting information services must be protected from interception or damage.
* Information assets must be maintained in accordance with appropriate mandatory procedures in place. As a minimum these procedures will recognize the criticality of the equipment and will comply with the vendor’s recommendations and specifications.
* Only authorized and qualified maintenance personnel must perform maintenance of the XXXX’s assets.
* Information assets used to support business activities outside of the XXXX’s premises must be made subject to the same type of authorization and security protection as that of on-site Information assets.
* Use of removeable media in the XXXX must be authourised by the Head of IT and only removeable media provided by IT can be used.
* IT personnel will carry out the removeable media activity for any approved user. Users are not allowed to make use of removeable media on their own
* No food, drink or smoking in the Comms Rooms in the Cornhill office.
* No cardboard or packaging should be stored in the Comms Rooms in the Cornhill office.
* The comms room must not be used as an office
* IT must ensure these removeable devices are physically secured, checked for malware and data copied in them are treated in line with the data classification policy.
* If circumstances demand, XXXX is at liberty to use all her monitoring systems both physical and logical to monitor the activities of staff, visitors, and consultants.
* All Information assets containing storage media (e.g., fixed hard drives) must be checked to ensure that any critical business information and licensed software are removed, securely overwritten or destroyed prior to disposal or re-use.

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. 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 |

## Enforcement

All staff of ZBL must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current ZBL 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 Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| CCTV | Closed Circuit TV |

# Document Management

## Document Revision Log

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

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

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

## Document Distribution

Distribution is to all staff