Visitors Access Procedure

*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 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

1.3.1 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

2.1 Visitors Access 4

2.2 Consultant Access 4

2.3 Access Review 4

3. Procedure Compliance & Enforcement 5

3.1 Compliance Measures 5

3.2 Enforcement 5

4. Glossary / Acronyms 6

4.1 Glossary / Acronyms 6

5. Document Management 7

5.1 Document Revision Log 7

5.2 Document Ownership 7

5.3 Document Coordinator 7

5.4 Document Approvers 7

5.5 Distribution 7

# Introduction

## Document Definition

This document is a Procedure.

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

## Objective

This document lists the steps to be followed when a visitor/consultant and staff without access card are to be granted access to XXXX office

## Scope

### Applicability to Employees

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

### Applicability to External Parties

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

### Applicability to Assets

This Procedure 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*
* *XXXX-POL-ALL-023 - Physical Security Policy*
* *XXXX-STD-ALL-017 - Physical Security Standard*

# Procedure Statements

## Visitors Access

1. Visitors approach the receptionist on the ground floor stating the details and who to see
2. Receptionists confirm from the system if the visitor has been booked for the visit by a staff, if not move to step 3
3. Receptionists contact the staff visitor is to see and get confirmation the visitor is expected
4. Receptionist takes down the visitors’ details and generates a paper card with visitor’s name.
5. The paper card is attached to a blue coloured lanyard and given to the visitor
6. Visitor will display this lanyard and card conspicuously
7. Staff the visitor want to see will come to the ground floor to escort the visitor into the office.
8. At the end of the visit, the staff will escort the visitor to the receptionist where the visitor’s lanyard and card will be handed over and the visitor leaves the premises

## Consultant Access

1. Receptionists contact the staff consultant is to see and get confirmation the consultant is expected
2. Consultant with long term access will be given a form granting them access to the facility for a maximum of one year
3. They will sign in for access card at the reception
4. Consultant for one off duties will only need to sign for their access cards at the reception
5. They will be issued a yellow coloured lanyard and access card to the required floor(s)
6. The yellow coloured lanyard and access card will be returned after completion of their task.

## Staff without their Access Cards

Staff who don’t have their access cards will be required to sign in at the reception and HR or member of the staff department will be contacted to identify the staff after which an access card will be issued by the receptionist

## Access Review

XXXX will carry out a review at least once a year on status of access cards issued to staff, visitors, and contractors. The review will also cover the access control system, closed circuit TV and the general physical environment managed by one 55 Fenchurch the landlord

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures 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.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| XXXX | XXXX |

# Document Management

## Document Revision Log

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

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

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

## Distribution

* *All Staff*