Third Party Access Request 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

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 4

2. Procedure Statements 5

2.1 Procedure Details 5

3. Third Access Request Procedures 6

4. Procedure Compliance & Enforcement 7

4.1 Compliance Measures 7

4.2 Enforcement 7

5. Glossary / Acronyms 8

5.1 Glossary / Acronyms 8

6. Document Management 9

6.1 Document Revision Log 9

6.2 Document Ownership 9

6.3 Document Coordinator 9

6.4 Document Approvers 9

6.5 Distribution 9

6.6 Appendix A 9

# 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

The Third-Party Access procedure sets out the conditions that are required to maintain the security of the bank’s information and information systems when third parties are involved in their operation. This may occur in at least four distinct circumstances:

* When third parties (for example contractors) are involved in the design, development or operation of information systems for the bank. There may be many reasons for this to happen, including writing and installing bespoke software, third party maintenance or operation of systems, to full outsourcing of an IT facility;
* When access to the bank’s information systems is granted from remote locations where computer and network facilities may not be under the control of the bank i.e Frontier
* When users who are not employees of the bank are given access to information or information systems i.e Auditors

Each of these circumstances involves a risk to the bank’s information, which should be assessed before the third party is granted access. Such access must be subject to appropriate conditions and controls to ensure the risk can be managed.

## 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*

# Procedure Statements

## Procedure Details

* All third parties who are given access to the bank’s information systems, whether suppliers, customers or otherwise, must agree to follow the bank’s information security policies. The bank will require external suppliers of services to sign a confidentiality agreement as provided by Legal to protect its information assets.
* The request must be sponsored by a department / unit in XXXX or and duly approved by the departmental head. Where hard copy access requests cannot be provided, email from the unit head will suffice.
* The System Owner will act as the sponsor for the Third Party where there is an approved need for Third Party Access. The System Owner (sponsor) will be expected to notify the IT service desk once the work has been completed.
* Third party access will be governed by formal written signed agreements. The Third Party Access form must be signed by all third parties prior to access being given if the third party do not already have an agreed agreement with the Bank. See Appendix A – Third Party Access Form. Also, the access details section of the form must be included in the helpdesk access request for all third parties
* Security and data controls will be agreed and defined in a contract with the third party as detailed in the DPIA
* All access will be using appropriate standards and technical solutions as defined by XXXX IT staff. This will be carried out in conjunction with the Information Security Officer (ISO).
* Third party users will be restricted to the minimum services and functions which are required to perform the specified tasks, as outlined by the System Owner (sponsor) in the original request for access.
* XXXX reserves the right to audit both the processes and systems of the third party, in so far as it relates to XXXX owned data. User’s systems may be audited to ensure no unauthorized activity is unnoticed. Any audit logs produced will be reviewed frequently.
* Appropriate protective monitoring techniques will be applied depending on the sensitivity of the data involved in the transactions.
* The Third Party is solely responsible for ensuring that any username and password that are granted remains confidential and is not used by unauthorized individuals.
* Third party connections must comply with requirements as stated in Service Level Agreements.
* Employees must use only the Bank’s official email accounts, to conduct the Bank’s business.
* XXXX will require Third Parties to undertake appropriate Information Security Awareness training sessions and to sign up to the XXXX Acceptable Usage Policy (AUP) in consideration to the outcome of the DPIA performed
* The third party connection may be disconnected without notice if a breach of security is suspected or if the connection is interfering with normal operation of the production systems.
* The Bank reserves the right to monitor activity and revoke access.
* On completion of the contract, the third Party must return all information facilities belonging to the Bank.

# Third Access Request Procedures

1. User/sponsor making the request for the third party access will send a mail/helpdesk request to the Head of IT listing the access level required and the applicable systems
2. The Head of IT will request from the user, evidence that the third party have signed an NDA and agreed with the information policy set of the bank. If not available, the Head of IT can send the third party access form in this procedure for the third party to complete
3. The Head of IT will grant approval to IT helpdesk (helpdesk@zenith-bank.co.uk) to grant the access
4. Helpdesk will grant the access and communicate the login details to the requesting officer for onward transmission to the third party

# 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

|  |  |
| --- | --- |
| ISO | Information Security Officer |

# 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

*Distribution is to all staff*

## Appendix A

**Appendix A – Third Party Access Form**

|  |  |
| --- | --- |
| Access to XXXXs information systems and network has been requested by : |  |
| Signature & Date |  |

**ACCESS DETAILS**

|  |  |
| --- | --- |
| **Access is granted to:**  [specify Name and Contact details of Company/Individual, including location] |  |
| **Access is granted in the form of:**  [specify access details e.g. Username/ Password] |  |
| Number of users: |  |
| Access is granted to the following data/ systems/device(s): |  |
| Remote access method granted will be:  [specify access details (e.g. VPN/dial-up))] |  |
| Domain/applications available via this system |  |
| Protection methods in use to protect connection/time i.e dedicated IP to be used by third party |  |
| Protection methods in use to protect domain/other application use i.e access to other domains/applications not allowed apart from the approved access granted |  |
| Protection methods in use to protect organizational sensitive data i.e sensitive data are protected through extra controls |  |
| Length of time access is for |  |

**SECURITY CONDITIONS**

* Access to XXXX systems and data is granted for approved purposes only. The use of this access for personal use or gain is strictly prohibited.
* Access to the Bank’s information & network facilities will not be provided until a signed copy of this contract has been returned to XXXX.
* The Third Party is permitted only to use access methods meeting appropriate protocols.
* The Third Party will inform the Bank in writing of appropriate staff changes in relation to access to XXXX systems.
* The Bank reserves the right to monitor activity, revoke access and audit contractual responsibilities.
* Where the Third Party has direct or indirect access to data or information owned by the Bank, this information must not be copied, divulged or distributed to any other party.
* On the completion of this contract the third Party must return all data belonging to XXXX.
* Any suspected security breaches or other incidents must be reported in a timely manner to the vendor’s contact person.
* The Third Party will always be held responsible for any activities that occur on the Bank’s network and applications using any unique user IDs granted.
* The Third Party is solely responsible for ensuring that any username(s) and password(s) that they are granted remain confidential and is not used by unauthorised individuals.
* The Third Party agrees that once access has been gained to the network, system or data, activities will be restricted to that system or data and to resolution of the issue(s) or provision of the agreed service that gave rise to the requirement for access on that occasion. These will be detailed in this agreement, or in an attached contract or Service Level Agreement.
* The Third Party shall not use, divulge or communicate any personal information including information relating to the Client's finances, business or commercial affairs, or information of a technical nature, made accessible to the supplier as a consequence of this agreement, which it shall treat as confidential and safeguarded accordingly.
* The Third Party shall ensure that its employees, agents, subcontractors and any third parties to whom data or information is disclosed or made accessible under this agreement are aware of the requirement to maintain the security and confidentiality of any such data and information
* Workstations/laptops that are used to display the bank’s data should be located in such a way that confidential information is not displayed to unauthorised persons or the general public.
* The Bank reserves the right to increase security thresholds if future security risks are identified.
* All Third party hosts connected to the Bank’s network must:
* Use the most up-to-date anti-virus/anti-spyware/anti-malware software available
* Be protected by a Corporate or private Firewall
* Be up to date with operating system patches
* Not be made available for use to unauthorised third parties
* Be available for inspection by IT Services or the Information Security Officer if requested.

(3RD PARTY COMPANY’S NAME AND ADDRESS)

**Signed for on behalf of 3rd PARTY**

**NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Of: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signed for on behalf of XXXX**

**NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Of: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Sponsor/ HOD: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Head, IT: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Information Security Officer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**