|  |  |
| --- | --- |
| **Document Name** | **Third Party Security Policy** |
| **Version** | **0.2** |
| **Last updated by** | **Anjaly T A** |
| **Approved By** | **Inderjit Singh Bedi** |
| **Released on** | **25-08-2022** |

Contents

[1. Overview 2](#_Toc61445282)

[2. Purpose 2](#_Toc61445283)

[3. Scope 3](#_Toc61445284)

[4. Privacy 3](#_Toc61445285)

[5. Policy Compliance 3](#_Toc61445286)

[6. Policy 4](#_Toc61445289)

# Overview

This document contains the code of conduct and information sharing with third parties that require any kind of integration or access to any of the services that are designed and implemented by the Xtracap organization.

# Purpose

This document describes the policy under which third party persons or organizations connect to or access network resources on Xtracap networks for the purpose of business-related transactions or other approved business transactions.

# Scope

All connections and network resources access between third parties that require access to non-public resources fall under this policy, regardless of what technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for Xtracap or to the Public Switched Telephone Network does NOT fall under this policy.

#### 3.1 Employees

This policy applies to all Employees, Contractors, and Third Party Employees, who use, process, and manage information and business processes of Xtracap.

#### 3.2 Records

Records being generated as part of this Policy shall be retained for the period of the partership. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

#### 3.4 Distribution and Maintenance

This Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the IT Infra team and system administrators.

# Privacy

This Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

# Policy Compliance

* 1. Compliance Measurement

This Policy shall be implemented by the IT Infra team and designated personnel (if any). This policy has full support from the executive steering committee and human resources. This policy is a living document and may be modified at any time by the IT manager, human resources, or the executive steering committee.

The IT Infra team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

# Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

# Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Policy

# 6.1 Pre-Requisites Security Review

# All new extranet connectivity will go through a security review with the Office of IT Manager. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

# 6.2 Third Party Connection Agreement

# All new connection requests between third parties and Xtracap require that the third party and representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by the IT Manager as well as a representative from the third party who is legally empowered to sign on behalf of the third party.  By signing this agreement, the third party agrees to abide by all referenced policies. The signed document is to be kept on file with the relevant extranet group.  All non-publicly accessible information is the sole property of Xtracap.

# 6.3 Business Case

# All extranet connections or network resource access must be accompanied by a valid business justification, in writing, that is approved by the third party. Typically, this function is handled as part of the *Third Party Agreement*.

# 6.4 Point of Contact

# The Third Party must designate a person to be the Point of Contact (POC) for the third party connection. The POC acts on behalf of the party, and is responsible for those portions of this policy and the “*Third Party Agreement”* that pertain to it. In the event that the POC changes, the relevant third party person or organization, must inform Xtracap promptly.

# 6.5 Establishing Connectivity

# All contracting authorities within that wish to establish connectivity or network resource access to a third party are to file an Extranet connectivity request with IT Manager accompanied by a “*Third Party Agreement”* signed by the third party person, organization, or rightful designee.  IT Manager will then engage the third party to address security issues inherent in the project. All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. All connectivity requests will have a specific beginning and ending date.  In no case will rely upon the third party to protect network or resources.  IT Manager will grant access to all approved resources and reserves the right to refuse access on the basis of legitimate security concern as decided by the IT Infra Lead.

# 6.6 Modifying or Changing Connectivity and Access

# All changes in access must be accompanied by a valid business justification, and are subject to security review.  The Xtracap team is responsible for notifying the third party person or organization and IT Manager when there is a material change in their originally provided information so that security and connectivity evolve accordingly.  Extensions will be granted on a case-by-case basis and must be requested in writing by the sponsoring contracting authority.

# 6.7 Terminating Access

# When access is no longer required, the concerned team within Xtracap must notify the IT Manager, who will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. IT Infra team must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be deprecated, and/or are no longer being used to conduct business or other approved business transactions will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct business or other approved business transactions necessitate a modification of existing permissions, or termination of connectivity, IT Manager will notify the POC of the concerned Xtracap team of the change prior to taking any action.