NTP CLOCK SYNCHRONIZATION POLICY

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Purpose

The purpose of this policy is to define the requirement that all network, server and cloud infrastructure in Trianz deploy a time synchronization service to ensure consistent usage of time for logging. The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source

2. Scope

This policy applies to all Trianz network, server, cloud infrastructure and communication services.

The requirements of this policy shall be implemented in all the systems under the ownership of Trianz, either on premises or on cloud and for all other Trianz managed systems, wherever applicable.

3. Policy Statements

- All systems covered by the scope of this policy must deploy clock synchronization technology to ensure consistent and usable timestamps for activity logging wherever feasible.
- At present, this means that all systems should use Trianz Network Time Protocol (NTP) to synchronize each server's clock with the NTP server.
- All Active Directory connected systems may synchronize time from their domain controllers if those domain controllers are synchronized to the central NTP server.

- To enhance security from threats contained within the firewall, the time server should use the access control and authentication facilities in NTP to restrict access to the service.
- For communicating with the time server for status and control it is best to use a secure protocol such as Secure Shell (Current latest version) and/or Simple Network Management Protocol (SNMP) current latest version (encrypted SNMP).
- Utilize at least two or more (three or more is strongly recommended) NTP servers with the lowest possible stratum to minimize/eliminate timing errors.
- Include at least two reference sources for the input. Having available several time sources, NTP can select the best candidates to build its estimate of the current time. Even when a network connection is temporarily unavailable, NTP can use measurements from the past to estimate current time and error.
- NTP is founded on the User Datagram Protocol (UDP), and is highly susceptible to IP spoofing, so blocking the non-authenticated ports at the firewall is essential for network perimeter security.
- Audit Logs with correct Clock synchronization shall help in investigations or as evidence in legal or disciplinary cases.
- Control of 12.4.4 – Control of Clock Synchronization remains the same for Standard 27018.
- NTP shall be synchronized as per the global standard.

4. Roles & Responsibilities

Sl. No	Item	Roles	Responsibility
1	Clock Synchronization	IS Operations/product teams	Shall have the responsibility and authority to cause this policy to be implemented and maintained. **As a Cloud Service Provider**: Shall provide information to Cloud Service Team about the Clock used and

			information on how client can synchronize the local clocks with the Cloud Service Clock **As a Cloud Service Customer**: Shall request the Cloud Provider about the Clock synchronization used for the Cloud Provider's Systems
2	Audit & Compliance	InfoSec Assurance	Annual Policy & Compliance Review

5. Exceptions(s)

There is no exception to this policy as of now. Exceptions to the NTP Clock Synchronization policy shall follow the Exception handling policy.

6. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Control	8.17 Clock synchronization Control The clocks of information processing systems used by the organization shall be synchronized to approved time sources	NTP Clock Synchronization Policy

Document Control

Owner:	CISO	Release ID:		NTPC-POL-0050

[For Trianz Process Improvement Group (TPIG) Purpose Only](#)

Version History

Ver. No.	Date	Author	Reviewer	Introduction/Reason for Change	Approver	Change Description
0.1	27-Apr-2018	Kamadev Pradhan	Gangadhar	Initial		Initial Draft
1.00	20-Jun-2018	Kamadev Pradhan		Approval for Baseline	Ganesh AJ	Baseline
2.00	25-Nov-2019	Vijaya Rajeswari Veldurthy	Phani Krishna, Pranesh Kulkarni	Updated to align to ISO 27017 and ISO 27018 Standard	Vivek Sambasivam	Roles and responsibilities as Cloud Provider and Cloud Customer updated Objective updated to align with ISO 27002
2.1	10-May-20	Balu Nair	Phani Krishna	Annual Review		Moved to the New template
3.0	14-May-20	Balu Nair	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
3.1	21-Jan-21	Karthik N	Phani Krishna	For Review		Updated the information classification Updated as per the

						Feedback from Pranesh.
4.0	21-Jan-21	Karthik N	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
5.0	30-Oct-21	Pranesh Kulkarni	Gangadhar Aka	For Review	Sivaramakrishnan	Baseline Review
5.0	23-Dec-21	Pranesh Kulkarni	Karthik N	Annual Review		No Changes
5.1	14-Mar-22	Sanjana	Karthik N	For Review	Sivaramakrishnan	The scope has been extended to products and services
6.0	18-Mar-22	Sanjana	Karthik N	For Approval	Sivaramakrishnan	Approved and Baselined
6.1	16-Feb-23	Balu Nair, Pallavi Chakrabarty	Karthik ,Vijaya R	Yearly Review		w template change
7.0	12-May-23	Balu Nair	Vijaya R	For Approval	Srikanth M	• Approved and Baselined
7.1	11-Feb-24	Shalini	Vijaya R	Yearly Review	Srikanth M	Mapped to new ISO 27k 22 Control
8.0	23-Feb-24	Shalini	Vijaya R	For Approval	Srikanth M	• Approved and Baselined
8.1	28-May-25	Vijaya	Balu		For Yearly Review	• Migrated to a new Template
9.0	29-May-25	Vijaya	Balu	Srikanth M	For Approval	• Approved and Baselined

TRIANZ

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com