NETWORK TIME SYNCHRONIZATION

The importance of accurate, stable, and reliable time is fast becoming one of the most important issues in the growing world of information security. Driven by regulatory compliance measures, along with the overall need for ensuring the confidentiality, integrity, and availability (CIA) of critical system resources, organizations are now paying much more attention to the concept of network time synchronization – the policies, procedures, and processes for deploying and maintaining what was just noted – accurate, stable, and reliable time. From health care to financial services – and many other industries and business sectors – having measures in place that effectively promote and support best practices for network time synchronization is a must, and I.T. professionals are quickly recognizing the importance. Imagine critical system resources that produce inaccurate time – or worse, no time – for audit trails, log files, and other important monitoring and oversight mechanisms. Not knowing the correct times and duration for files being accessed, software changes made, or any other number of activities can lead to serious security and legal issues, all of which can be very costly, both financially and operationally. Specifically, serious legal implications can arise from organization who embark on time manipulation techniques – both intentionally (i.e., out of need to cover up alleged unauthorized activities on system resources) and unintentionally (i.e., failing to implement adequate network time synchronization measures on system critical system resources).

But with many of today's current and emerging technologies in place, the ability to effectively monitor and oversee day-to-day operational activities on critical system resources is now a reality, provided that these very systems are enabled with accurate and reliable stable time. File Integrity Monitoring (FIM) solutions, change detection software, Intrusion Detection and Prevention Systems (IDPS), and many other traditional system resources (i.e., firewalls, operating systems) – they're only as good as the settings and configurations applied to them. Thus, a core requirement in provisioning and hardening critical system resources must always include accurate, stable, and reliable time. And while I.T. engineers have always focused on access rights and other essential hardening techniques – and these are still very critical, no question about it - network time synchronization is now more important than ever.

Keep in mind that network time synchronization and the concept of accurate, stable, and reliable time serves the following purposes:

1. Event Synchronization – Technically speaking, allows for actions to be executed – or simply stated – events to occur at specific time as scheduled, such as starting, stopping, continuously running, etc.
2. Interoperability – Allowing system resources to coordinate, and ultimately work and function with other systems without any restrictions, regardless of location, time zones, etc.
3. Evidentiary Matter (time and date stamping (i.e., digital timestamps), log files, audit trails, etc.) - Information identifying when specific events occur, thus providing critical digital timestamp (date and time of day) information, which ultimately allows for evidentiary matter produced, such as log files, audit trails. etc.
4. Risk Awareness – Helps better assess one's overall risk assessment platform, specifically relating to regulatory compliance risks, which often mandate not only strict time synchronization

requirements, but also that of other critical I.T. controls, such as access control, network monitoring, logging, etc.

5. CIA – Ultimately, implementing comprehensive time synchronization measure helps ensure the confidentiality, integrity, and availability (CIA) of an organization's information systems architecture.

And when speaking about network time synchronization, it's important to note that Network Time Protocol – simply known as NTP – is the networking protocol for clock synchronization that uses UDP port 123. NTP is just the protocol – secure, accurate, reliable, and stable time still has to be acquired – and that generally comes from International Atomic Time (TAI) or Coordinated Universal Time (UTC) time sources, often from national physical laboratories. And to get time from a trusted source, you'll need an NTP time server, which then becomes your single point of time that's ultimately distributed to other systems in one's environment. As for how time is received, it's either by a radio transmission or GPS enabled signals. And finally, NTP employs a stratum (i.e., plural is "strata") platform whereby time is pushed down from one stratum to the next, which prevents the actual NTP server itself from being asked for numerous requests for time. Thus, the term "stratum" defines the distance from the original time source within your NTP architecture.

Network Time Synchronization Policy and Procedures

Title	**[company name] Network Time Synchronization Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Use of Software
Approval Date	TBD
Purpose of Document	To implement comprehensive Network Time Synchronization policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's NTP policies.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Network Time Synchronization policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Network Time Synchronization policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] system resources.

1.0 Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system resources".

1.0 Policy