GUIDELINE ON SYSTEM CLOCK SYNCHRONISATION - *DRAFT*

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA (IIUM)

SECTION 1: INTRODUCTION

1.1 OBJECTIVE

To ensure the highest standards of security, accuracy, reliability, and regulatory compliance through precise and consistent timekeeping across all University systems. Accurate time synchronisation is critical for maintaining the integrity of security logs, coordinating system operations, and meeting regulatory requirements.

1.2 SCOPE

These guidelines apply to all systems, devices, and applications within the University, including on-premises, virtual, and cloud-based environments. It mandates consistent time synchronisation practices across all networked equipment—such as servers, virtual machines, cloud instances, workstations, and time-dependent devices—to ensure operational integrity, security, and regulatory compliance

1.3 APPLICABILITY

These guidelines apply to all staff, contractors, and third-party service providers who manage or utilise University systems. They ensure that all relevant parties adhere to the prescribed time synchronisation protocols, thereby supporting the University's overall security posture and operational efficiency.

1.4 RELATED POLICIES/PROCEDURES

1.4.1 IIUM ICT Regulation

1.4.2 ISO/IEC 27001:2022: Ensure compliance with international standards for information security management, specifically Control 8.17 on clock synchronisation.

1.4.3 Personal Data Protection Act 2010 [Act 709]: Accurate timekeeping is essential for data integrity and audit trails, supporting data protection law compliance.

1.5 TERMS AND DEFINITIONS

Terms/Abbreviations	Definitions
IIUM	International Islamic University Malaysia
KCDIOM	Kulliyyah, Centre, Division, Institute, Office or Mahallah
ITD	Information Technology Division
ITD Director	Director of Information Technology Division
NTP	Network Time Protocol. This protocol ensures precise and consistent timekeeping across in a network, which is essential for accurate logging, robust security measures, and the seamless operation of distributed applications
System Administrator	A person responsible for the management of the networked systems, devices, and applications.

SECTION 2: EXPLANATION OF THE IMPLEMENTATION OF THE GUIDELINES

2.1 GUIDELINES

2.1.1 All systems, devices and application within the University must synchronise their clocks with a reliable, secure, and accurate time source. Continuous time synchronisation is mandatory to maintain consistency and support the University's security, reliability, and regulatory compliance objectives. This policy is integral to preventing security incidents, ensuring accurate transaction records, and facilitating forensic investigations.

2.1.2 This guideline shall be implemented in accordance with IIUM's ICT Security Procedure in compliance with ISO 27001:2022 requirements to ensure confidentiality, availability and integrity in all processes. All processes, decisions, and activities under this policy/guideline must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

2.2 INTRODUCTION

Accurate and consistent time synchronisation across all University systems is essential to ensure operational reliability, robust cybersecurity, and compliance with regulatory requirements. Time synchronisation underpins critical functions, including security logging, incident investigation, system coordination, and audit processes. Discrepancies in timestamps can compromise forensic analysis, disrupt automated processes, and lead to non-compliance with legal and institutional obligations.

The University mandates the implementation of a standardised time synchronisation framework to maintain uniformity across all networked devices, servers, and applications. This guideline establishes the protocols and responsibilities necessary to achieve precise timekeeping, safeguard system integrity, and ensure adherence to data protection, financial regulations, and other statutory requirements.

By applying the standard time synchronisation practices, the University strengthens its security posture, enhances operational efficiency, and upholds accountability across its digital infrastructure. This document defines the procedures and standards required to maintain synchronised timekeeping in alignment with institutional policies and industry best practices.

2.3 PLANNING

This section defines the strategic approach and architectural framework for achieving and maintaining accurate time synchronisation across the University's server, in accordance with ISO/IEC27001:2022 Control A.8.15.

2.3.1 Target Time Synchronisation Architecture

The Time sources for the clock synchronisation are below:

No.	Time server address	Description	Configuration Priority
1	ntp1.sirim.my	SIRIM official time server	1 (main)
2	my.pool.org	Time server from pool.ntp.org	2

2.3.2 **Traceability to National Standards**

All time synchronisation shall be traceable to national and international time standards. The chosen time sources, whether internal or external during the transitional phase, must provide verifiable proof of their accuracy and legitimacy for regulatory and audit purposes.

2.4 IMPLEMENTATION

2.4.1 System Administrators across all KCDIOs are responsible for configuring all systems, devices, and applications under their purview to synchronise with the designated internal Stratum 2 NTP servers.

2.5 MONITORING

22.5.1 Continuous monitoring is essential to ensure the ongoing effectiveness of the time synchronisation guidelines. The monitoring system shall generate regular reports on synchronisation performance and alert the ITD to any deviations or failures.

2.6 COMPLIANCE

32.6.1 The Director of Information Technology Division holds the responsibility for the implementation of this guideline and shall take necessary actions in the event of violation of this guideline.

SECTION 3: ADMINISTRATION OF THE GUIDELINES

3.1 OWNERSHIP OF THE GUIDELINES

3.1.1 The Director of the Information Technology Division (ITD) is designated as the official owner of this guideline. The Guideline Owner holds ultimate responsibility for its content, approval, and overall effectiveness.

3.2 ROLES AND RESPONSIBILITY OF THE OWNER OF THE GUIDELINES

3.2.1 Acts as the ultimate owner and approver of this guideline.

3.2.2 Allocates necessary resources for its implementation and maintenance.

3.2.3 Holds overall accountability for University-wide compliance.

3.3 REVIEW AND REVISION PROCESS

3.3.1 This guideline shall be reviewed periodically, or as needed based on changes, to ensure its continued relevance and effectiveness.

SECTION 4 : REFERENCE DOCUMENT

4.13 REFERENCE

The following documents were referenced in the creation of this guideline and provide the foundational requirements and context.

4.1.1 IIUM ICT Policy
4.1.2 ICT regulations
4.1.3 IIUM Information Management Policy
4.1.4 IIUM ICT security procedure
4.1.5 IT Infrastructure Lihrary(ITIL)
4.1.6 Control of Business IT(COBIT)
4.1.7 Personal Data Protection Act 2010 [Act 709]