P-17 IT and Digital Systems Policy

International Federation of Arbitration (IFA)

1. Definition
This Policy establishes the framework governing the management, use, security, and maintenance of information technology systems and digital infrastructure within the International Federation of Arbitration (IFA), ensuring efficiency, reliability, and protection of digital assets.

2. Objective
The objective of this Policy is to ensure the secure and effective use of IT systems, support operational activities, protect digital information, and maintain continuity of digital services.

3. Scope of Application
This Policy applies to all IT systems, digital platforms, software, hardware, networks, and users, including employees, members, and authorized stakeholders interacting with the Federation's digital infrastructure.

4. Governing Principles
This Policy is based on the principles of security, reliability, accessibility, efficiency, accountability, and alignment with international IT governance standards.

5. IT Infrastructure Management
All IT infrastructure shall be managed to ensure availability, performance, scalability, and security in support of the Federation's operations.

6. System Access and Authorization
Access to systems shall be granted based on roles and responsibilities, using secure authentication mechanisms and access controls.

7. Acceptable Use of IT Systems
Users must utilize IT systems for authorized purposes only and must not engage in activities that compromise system integrity or security.

8. Cybersecurity Measures
Appropriate cybersecurity measures shall be implemented, including firewalls, encryption, antivirus systems, and intrusion detection mechanisms.

9. Data Protection Integration
IT systems shall be designed and managed in alignment with the Data Protection and Privacy Policy to ensure data security and confidentiality.

10. System Maintenance and Updates
Regular maintenance, updates, and upgrades shall be conducted to ensure system functionality, security, and performance.

11. Backup and Recovery
Data backup procedures and disaster recovery plans shall be established to ensure business continuity in case of system failure or data loss.

12. Monitoring and Logging
System activities shall be monitored and logged to detect unauthorized access, ensure accountability, and support security investigations.

13. Incident Management
IT incidents, including system failures or security breaches, must be reported, documented, and managed promptly to minimize impact.

14. Use of External Systems and Services
Use of third-party systems or cloud services must comply with security requirements and be approved by the Federation.

15. User Responsibilities
All users are responsible for protecting their access credentials, complying with IT policies, and reporting any suspicious activities.

16. Compliance with Standards
IT practices shall comply with recognized international standards and applicable regulations.

17. Violations
Violations include unauthorized access, misuse of systems, cybersecurity breaches, or non-compliance with IT procedures.

18. Sanctions
Sanctions may include restriction of access, disciplinary action, or legal consequences depending on the severity of the violation.

19. Review and Amendment
This Policy shall be reviewed periodically to ensure alignment with technological advancements and emerging security threats.

20. Annexes
Annexes may include IT usage guidelines, security protocols, incident response procedures, and system architecture documentation.