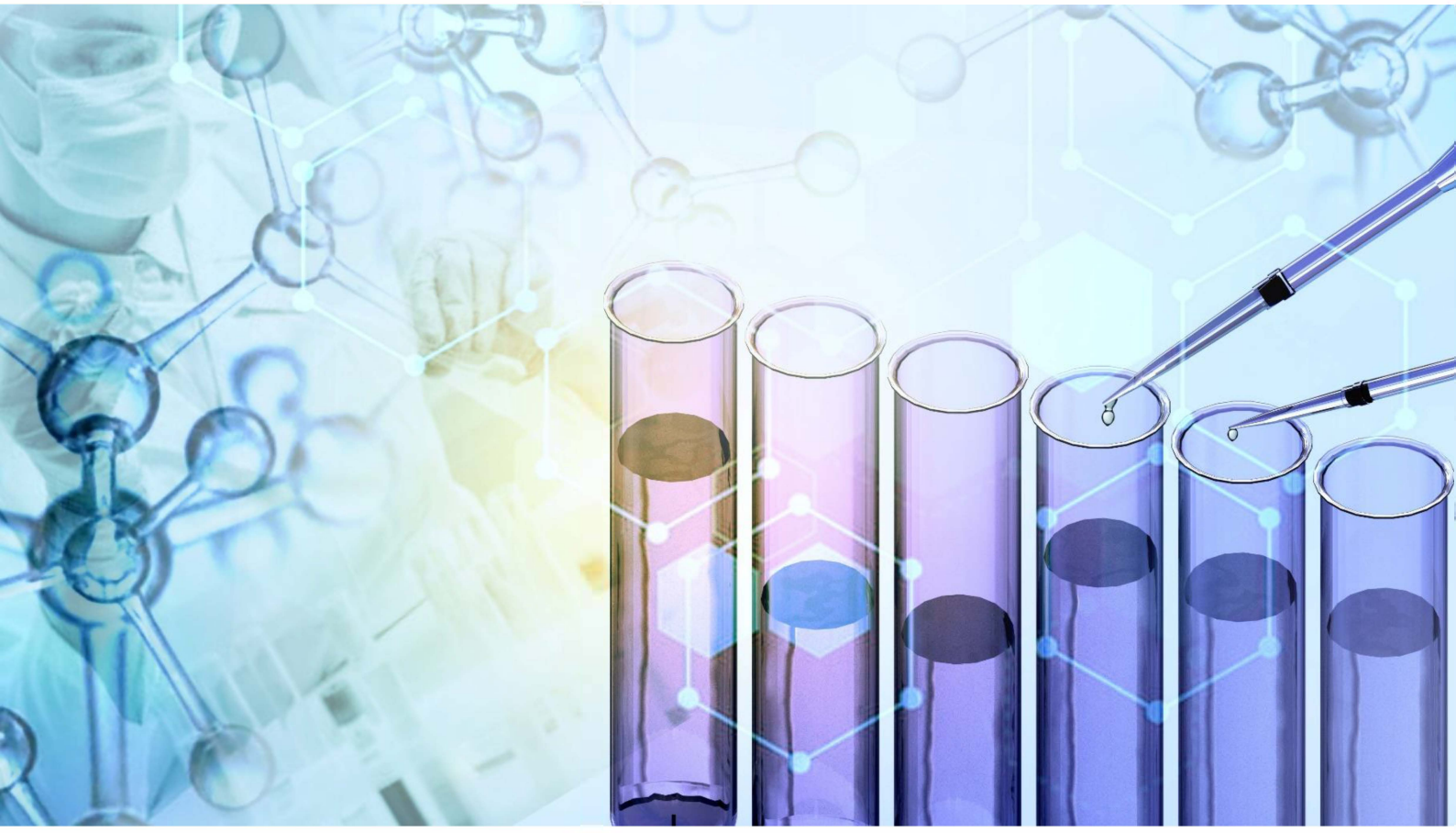
OECD Position Paper on Good Laboratory Practice and IT Security

Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 25



OECD

Series on Principles of Good Laboratory Practice and Compliance Monitoring
No. 25

OECD Position Paper on Good Laboratory Practice and IT Security

Please cite this publication as:

OECD (2024), *OECD Position Paper on Good Laboratory Practice and IT Security*, OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 25, OECD Publishing, Paris.

About the OECD

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organisation in which representatives of 38 countries in North and South America, Europe and the Asia and Pacific region, as well as the European Union, meet to co-ordinate and harmonise policies, discuss issues of mutual concern, and work together to respond to international problems. Most of the OECD's work is carried out by more than 200 specialised committees and working groups composed of member country delegates. Observers from several Partner countries and from interested international organisations attend many of the OECD's workshops and other meetings. Committees and working groups are served by the OECD Secretariat, located in Paris, France, which is organised into directorates and divisions.

The Environment, Health and Safety Division publishes free-of-charge documents in twelve different series: **Testing and Assessment**; **Good Laboratory Practice and Compliance Monitoring**; **Pesticides**; **Biocides**; **Risk Management**; **Harmonisation of Regulatory Oversight in Biotechnology**; **Safety of Novel Foods and Feeds; Chemical Accidents; Pollutant Release and Transfer Registers; Emission Scenario Documents; Safety of Manufactured Nanomaterials;** and **Adverse Outcome Pathways.** More information about the Environment, Health and Safety Programme and EHS publications is available on the OECD's World Wide Web site (https://www.oecd.org/en/topics/chemical-safety-and-biosafety.html).

This publication was developed in the IOMC context. The contents do not necessarily reflect the views or stated policies of individual IOMC Participating Organizations.

The Inter-Organisation Programme for the Sound Management of Chemicals (IOMC) was established in 1995 following recommendations made by the 1992 UN Conference on Environment and Development to strengthen co-operation and increase international co-ordination in the field of chemical safety. The Participating Organisations are FAO, ILO, UNDP, UNEP, UNIDO, UNITAR, WHO, World Bank, Basel, Rotterdam and Stockholm Conventions and OECD. The purpose of the IOMC is to promote co-ordination of the policies and activities pursued by the Participating Organisations, jointly or separately, to achieve the sound management of chemicals in relation to human health and the environment.

Foreword

This position paper was developed by the OECD Working Party on Good Laboratory Practice (GLP) via a drafting group led by Denmark (Medical Products) and consisting of Austria, Belgium, Canada, France (Medical Products), Germany and Switzerland. The document draws upon a publication developed on cyber security and Good Clinical Practice (GCP) at the level of the European Union. The document was reviewed and endorsement by the Working Party on Good Laboratory Practice. This document is published under the responsibility of the Chemicals and Biotechnology Committee which agreed to its declassification.

Table of contents

About the OECD 3

Foreword 4

Considerations regarding IT security and GLP test facilities 6

1. Introduction 6
2. Scope 6
3. Ongoing security measures and GLP responsibilities 6
4. Physical security 7
5. Firewalls 7
6. Vulnerability management 7
7. Platform Management 8
8. Bidirectional devices (e.g. USB) 8
9. Anti-virus software 8
10. Penetration testing 8
11. Intrusion detection and prevention 8
12. Internal activity monitoring 9
13. Security incident management 9
14. Authentication method 9
15. Remote authentication 9
16. Password policies 9
17. Password confidentiality 10
18. Inactivity logout 10
19. Remote connection 10
20. Protection against unauthorised back-end changes 10
21. Backup 10
22. Standard Operating Procedures (SOP) 11

Considerations regarding IT security and GLP test facilities

1. Introduction

GLP data are more and more generated and retained in electronic format. Measures of IT security aim to protect electronic GLP data and applications against the specific hazards encountered in the computerized environment.

Threats and attacks on systems containing GLP data and corresponding measures to ensure security of such systems are constantly evolving, especially for systems and services being provided over or interfacing the internet.

Handling of IT security may be outsourced by test facilities to external service providers. However, the responsibility remains with the test facility. The recommendation and advice of vendors of operating systems and platforms should be carefully considered and applied where appropriate.

2. Scope

This position paper concerns electronic GLP data and linked computerised systems hosted in servers and subject to computerised corruptions.

The concepts in this document for “test facilities”, “Test facility management” and “study directors”, would equally apply to “test sites”, “test site management” and “principal investigators”, where delegated study phases are conducted as part of a multisite study (these terms are defined in the GLP Principles).

3. Ongoing security measures and GLP responsibilities

Test facility management should maintain a security system that prevents unauthorised access and ensures availability to GLP data. Procedures and measures to ensure IT security should be based on the risk and consequence of system malfunctions or internal or external deliberate or undeliberate actions that might adversely affect the integrity of GLP data.

4. Physical security

Servers, computers, infrastructure and media hosting GLP data and computerised systems relevant to GLP should be physically protected against unauthorised access, damage and loss. The extent of security measures depends on the criticality of the data.

Test Facility management should ensure an adequate level of security for data centres as well as for local hardware such as servers, computers, tablets, phones, hard disks and USB drives.

At data centres hosting GLP data and applications, physical access should be limited to the necessary minimum. A two-factor authentication can be used. Data centres should be constructed to minimise the risk and impact of natural disasters, there should be pest control and effective measures against fire (e.g. cooling, fire detection and fire suppression), flooding and any other cause that could alter data. There are generally emergency generators and uninterruptible power supplies (UPS) together with redundant internet protocol providers. In case the data centre is of type `co-location´, the servers should be locked up and physically protected (e.g. in cages) to prevent access from other users (`co-location´ means date centres where the hosted hardware belongs to several organisations that have access to the server rooms).

Preferably, data are replicated at an appropriate frequency from a primary data centre to a secondary failover site at an appropriate physical distance to minimise the risk that the same fire or natural disaster destroys both data centres. A disaster recovery plan should be in place and tested.

5. Firewalls

In order to provide a barrier between a trusted internal network and an untrusted external network and to control incoming and outgoing network traffic (from certain IP addresses, destinations, protocols, applications, or ports etc.), effective firewalls are implemented. Firewall rules should be defined as strict as practically feasible, only allowing necessary and permissible traffic.

As firewall rules tend to be changed or become insufficient over time (e.g. as software vendors and IT technicians need certain ports to be opened due to installation or maintenance of applications, or as cyber threats evolve), they are periodically reviewed. This review should ensure that actual firewall rules continue to be set as tight as possible.

6. Vulnerability management

Critical vulnerabilities in operating systems and platforms can be exploited to give unauthorised individuals privileged access to systems, and to modify or delete data and make data inaccessible to legitimate users. Such exploits are seen in operating systems for servers, computers, tablets, mobile phones and routers as in platforms for databases etc. While these operating systems and platforms are under support, the vendors frequently release security patches to close these vulnerabilities. Consequently, relevant critical security patches for platforms and operating systems have to be applied in a timely manner (immediately is recommended).

Systems which are not security patched in a timely manner constitute a major risk for loss of data integrity. Where relevant, such systems have to be isolated from computer networks and the internet.

7. Platform Management

Operating systems and platforms for critical applications and components should be updated in a timely manner, in order to prevent their use in an unsupported state.

Unsupported platforms and operating systems, for which no security patches are available, are exposed to a higher risk of vulnerability. Validation of applications on new operating systems and platforms and of the migration of data should be planned ahead and completed in due time.

Unsupported platforms and operating systems should be isolated from computer networks and the internet.

8. Bidirectional devices (e.g. USB)

Bidirectional devices (e.g. USB) or other portable media or devices may have been used outside the test facility and could possibly compromise the system. Therefore, they should be strictly controlled as they may intentionally or unintentionally introduce malware and impact data integrity and availability.

9. Anti-virus software

Anti-virus software should be installed and activated on systems used in GLP, as appropriate. The anti-virus software should be continuously updated with the most recent virus definitions in order to identify, quarantine, and remove known computer viruses. This process should be monitored.

10. Penetration testing

For systems facing the internet, penetration testing have to be conducted at regular intervals in order to evaluate the adequacy of security measures taken and to identify vulnerabilities in system security, including the potential for unauthorised parties to gain access to and control the system and its data. Vulnerabilities identified, especially those related to a potential loss of data integrity, should be addressed and mitigated in a timely manner.

11. Intrusion detection and prevention

An effective intrusion detection and prevention system has to be implemented on systems facing the internet in order to monitor the network for intrusion attempts from external parties and for the design and maintenance of effective preventive measures.

Threats via wireless connections have to be considered risk-based and may require a similar approach.

12. Internal activity monitoring

An effective system, within the framework given by national labour legislation, for detecting unusual or risky user activities (e.g. shift in activity pattern) have to be in place.

13. Security incident management

Test facilities should work according to a procedure that defines and documents security incidents. Such incidents could be addressed in terms of criticality, and where applicable, implements effective corrective and preventive actions to prevent recurrence. In cases where data have been, or may have been, compromised, the procedures should include requirements to report security incidents to relevant parties where applicable. When using a service provider, the service level agreement should ensure that incidents are escalated to the Test Facility Management in a timely manner in order for the Test facility Management to be able to report serious breaches to all relevant parties (study directors, sponsors, archivist …).

14. Authentication method

The method of authentication in systems should identify users with a high degree of certainty. A minimum acceptable method would be by means of a user identification and password. The need for more stringent authentication methods should be determined based on a risk assessment of the criticality of the data, and might include authentication methods, such as two-factor authentication.

Two-factor authentication implies that two of the following three factors be used:

- something you know, e.g. a user identification and password
- something you have, e.g. a security token, a certificate or a mobile phone and an SMS pass code
- something you are, e.g. a fingerprint or an iris scan (biometrics)

User accounts are automatically locked after a pre-defined number of successive failed authentication attempts, either for a defined period of time, or until they are re-activated by a system administrator after appropriate security checks.

15. Remote authentication

Remote access to GLP data and application, e.g. to cloud-based systems, raises specific challenges. The level of security should be proportionate to the criticality of the data (e.g. data required to reconstruct the GLP studies) and to the access rights to be granted (read-only, write or even 'admin' rights). A risk-based approach should be used to define the type of access control required, depending on the level of risk.

16. Password policies

Formal procedures for password policies should be implemented. The policies should include but not necessarily be limited to length, complexity, expiry, login attempts, and logout reset. The

policies should be enforced by systems, verified during system validation, included in periodic reviews of the system validation and specifically addressed after detection of intruders. The password rules aim to prevent intrusion.

17. Password confidentiality

Passwords should be kept confidential. Passwords initially received from the system or from a manager or system administrator have to be changed by the user on their first connection to the system. This should be mandated by the system.

18. Inactivity logout

Systems including an automatic inactivity, which logs out a user after a defined period of inactivity, could be considered. In such a case, the user should not be able to set the inactivity logout time (outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a full re-authentication is required (e.g. password entry).

19. Remote connection

When remotely connecting to systems over the internet, a secure and encrypted protocol (virtual private network (VPN) and/or hypertext transfer protocol secure (HTTPS)) have to be used.

20. Protection against unauthorised back-end changes

The integrity of data has to be protected against unauthorised back-end changes made directly on a database by a database administrator. A method to prevent such changes could be by setting the application up to encrypt its data on the database or by storing data un-encrypted with an encrypted copy. In either case, the database administrator cannot be identical to the administrator of the application.

21. Backup

Backups are made, retained and stored following established procedures to ensure that GLP data can be restored in case data has been accidentally or deliberately changed or deleted, lost as the result of a hardware malfunction or corrupted, e.g. as the result of a cyber-attack. The frequency, retention and safe storage of backups is critically important to the effectiveness of the process to mitigate these incidents. Backups are made at suitable intervals (e.g. hourly, daily, weekly and monthly) and their retention (e.g. a week, a month, a quarter, forever) should be determined through a risk-based approach. Backups are not be stored at the same physical location, on the same logical network or behind the same firewall as the original data in order to avoid simultaneous destruction or alteration.

Depending on the timely requirements for disaster recovery after an incident, applications and system configurations may also need to be backed up, as it may otherwise take a long time to re-establish services.

Restoration of data and potentially applications and configurations from backup should be tested.

22. Standard Operating Procedures (SOP)

Procedures/policies should be in place describing what IT security measures are in place and taken by the test facility. It should also be clearly described how the facility will handle any IT security breach and the facility should alert its national GLP compliance monitoring authority in case of any IT security issues and data loss/hacks.

OECD Position Paper on Good Laboratory Practice and IT Security

Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 25

Data generated according to Good Laboratory Practice (GLP) are increasingly generated and retained in electronic format. Measures of IT security aim to protect electronic GLP data and applications against the specific hazards encountered in the computerised environment. Threats and attacks on systems containing GLP data and corresponding measures to ensure security of such systems are constantly evolving, especially for systems and services being provided over or interfacing the internet. Handling of IT security may be outsourced by test facilities to external service providers. However, the responsibility remains with the test facility. This position paper provides an overview of considerations regarding IT security and GLP test facilities.