SOP 0019 - Information Security Safeguards

STANDARD OPERATING PROCEDURE
Security Safeguards

SOP Number	105
Version Number	1.1
System Level/Applicable to	Digital Solutions, Operations
Supersedes	
Effective Date	2020-01-08
Number of Pages (including cover)	4

Site Approval/Authorization to Adopt

Name	Jayson To	**Title**	Digital Solutions - Service Delivery Manager
Signature		**Date**	2020-01-08

Name		**Title**	
Signature		**Date**	

Document History

Version	Summary of Changes Made	Effective Date
1	Original document.	
1.1	Updated to reflect UBC Information Security Standards, patching schedule, renamed to Digital Solutions.	April 20, 2021

1. **PURPOSE**

    a. This Standard Operating Procedure (SOP) describes the Digital Solutions platforms and personal information collected and stored by the data information systems which will be protected by security safeguards to protect again loss, theft, unauthorized access, disclosure, copying, use or modification of data.

1. **SCOPE**

    a. This SOP is applicable to all data collected by Digital Solutions platforms in custody of UBC Faculty of Medicine.

1. **RESPONSIBILITIES**

    a. IT System Administrators (server and application administrators) are responsible for ensuring a high level of physical, technical and organization security for all data in its custody, meeting or exceeding applicable institutional requirements for information security standards.

    a. Application administrators are responsible for the Digital Solutions data information application systems that are operated natively or through various container technologies. This includes monitoring, applying application security patches and upgrades in a timely manner that is compliant with UBC Information Security Standard M5 - Vulnerability Management.

    a. Server administrators are responsible for the maintenance and support of the server operating systems and middleware technologies including ongoing monitoring, applying security patches and upgrades in a timely manner that is compliant with UBC Information Security Standard M5 - Vulnerability Management.

2. DEFINITIONS

    a. **Personal Information:** is any recorded information on an identifiable individual. This may include, but is not limited to an individual's name, address, e-mail address, telephone number, age, identifying number, fingerprints, blood type, health care history, education, financial, criminal or employment history. Additional information can be found on UBC Information Security Standard U1 - Security Classification of UBC Electronic Information.

3. PROCEDURES

    a. **General Privacy and Security Guidelines**

i. Monitor developments in privacy legislation, privacy enhancing technologies and public opinion, and adapting to conform as necessary.

i. Meet recognized standards of physical, technical, and procedural data protection and security.

i. Foster transparency and accountability and increase awareness of privacy principles, policies and procedures.

i. Support controlled access to, and responsible use of, personal information.

b. Physical Safeguards

i. Digital Solutions platforms are hosted at the University of British Columbia (UBC) EduCloud Server Services at the University Data Center, 2405 Wesbrook Mall, Vancouver, BC, V6T 1Z3.

i. The University Data Center maintains a secure physical area with several layers of physical protection, including locked and alarmed premises, monitored electronic access and video surveillance at entrances. The premise is accessible by authorized UBC personnel through card access.

c. Technical Safeguards

i. Digital Solutions system architecture is designed to meet health authorities and UBC Information Security Standards.

i. Digital Solutions system architecture is designed as such that all internet facing servers are placed in a Demilitarized Zone (DMZ) as outlined in UBC Information Security Standard M10 - Internet-facing Systems and Services.

i. User access to the information stored on Digital Solutions platforms is based on role-based access model as outlined in UBC Information Security Standard M2 - User Account Management.

i. Administrative access (System and Application administrators) to Digital Solutions platforms is through the UBC MEDVPN pool.

i. Server and application data backups follow the Educloud local and remote backup policy which provides a crash consistent backup taken every night and copied to a remote location on the same day. The local backup retention is 28 daily while remote backup retention is 28 daily, 12 weekly and 12 monthly.

d. Organization Safeguards

i. Server and application systems administrators personnel must undergo the UBC Privacy and Information Security - fundamentals training.

i. External third party vendors must sign the Health Organization Privacy Compliance Agreement and Privacy Schedule and the UBC Security and Confidentiality Agreement - Supplementary Agreement.

i. External third party vendors are provided access to data on an "as needed" basis as per UBC Information Security Standard M2 - User Account Management. Only a small number of specially trained programmers involved in the frontend and backend application are authorized to handle the data as per UBC Information Security Standard M3 - Privileged Account Management.

i. Researchers wishing to use Digital Solutions research platforms must agree to the Researcher Confidentiality Undertaking and Terms of Use, binding them to conditions governing use of the data, security arrangements, assurances regarding disclosure, and requirements to return/destroy any copies of the data.

i. In case of a suspected breach of the Terms of Use, procedures will be followed as outlined in the Incident Management SOP.

a. **Safeguards for Transfer of Data**

i. Encryption of data deployed will meet the following standards:

1. SSL 3.0 using algorithm is AES

1. Key strength is 256 bit or greater

a. **Application Monitoring and Patching by Systems and Application Administrators**

i. Periodic infrastructure assessments and patches (operating system, middleware, databases) will be performed on a monthly basis, on the second Tuesday of every month to ensure the applications are up to date and secure. Off-cycle patches will be applied based on the criticality of the vulnerabilities as per UBC Information Security Standard M5 - Vulnerability Management.

i. The primary patching mechanism will be the Ivanti tool offered through UBC IT. All virtual servers in Educloud have the Ivanti agent installed to comply with the Digital Solutions server patching SOP.

i. Patches will be deployed to the development and testing environments first where applicable, to ensure the updates do not conflict with the production application ecosystem.

i. Application service owners or delegates will perform testing and validation of the changes and approve the deployment of these changes to the production environments.

i. Patches to the development and testing environments will be deployed on the Thursday following "Microsoft Patch Tuesday" and if successful, production deployment will occur on the Friday evening of the same week.

i. Systems and applications are monitored through PRTG for performance monitoring including but not limited to system and application uptime and other key processes.

a. **Log Monitoring and Audits**

i. Log Monitoring and audit procedures will be implemented according to the UBC IT patching and logging standard. Currently, servers provisioned through Educloud include 30 days of log retention.

1. **REFERENCES**

a. UBC Information Security Standards (revised), January 2021

a. Privacy Impact Assessment, 2019-121

a. Document 500: System Description, Security Threat Risk Assessment