DI-r Process:	**DIR Privileged Access Management Process**		
DI-r Process No.:	**DIR-PRC-001**		
Owner of Process:	**Coordinator, DIPACS ITS Department**		
SLT Sponsor:	**Manager, DIPACS ITS Department**		
Approval Date: **TBD**	**Effective Date:** TBD	**Reviewed Date:** -	**Revised Date:** -
Parent Standard:	ITS-STD-005	ITS Privileged Access Management Standard	
This process applies to:	Any individual or organization that users the DI-r Systems with a privileged account.		

1. PURPOSE

Privileged access provides abilities greater than those of a standard user, typically used to perform administrative duties within a system, such as system configuration changes, system updates/patches, user account management, etc.

The purpose of this process is to support the ITS Privileged Access Management Standard (ITS-STD-005) to reduce organizational risk and ensure the appropriate management of privileged access. Such risks include, but are not exclusive to:

- Unauthorized access to financial, personal health information, personal information or corporate information for personal benefit
- Privacy breaches, possible IPC orders, fines, investigations and / or prosecutions
- Identity theft
- Attack on systems i.e. denial of service
- Legislative and Regulatory non-compliance
- Legal action against the hospital
- Disruption to clinical care processes or business functions of the hospital
- Reputational damage to the hospital in the event of privacy and / or security breach, theft, or other adverse effect
- Financial exposure, including but not limited to, insurance coverage, liabilities, claims, losses, damages, expenses, legal fees

2. VALUE TO ORGANIZATION

The value of the Privileged Access Management Process is to:

- Establish a standard consistent approach to manage privileged access
- Mitigate risk to the organizations services, systems, confidential information and processes
- Maintain the security, integrity and availability of hospital systems
- Provide an auditable process to the management of privileged access
- Reduce privileged level access to only those that require such access based on the authorized job function or business needs
- Educate business, system and ITS service owners of their accountability and responsibilities for managing privileged access
- Develop accountability to business, system, and ITS service owners to manage privileged access

3. PROCESS PRINCIPLES

Principle 1: A standard, consistent approach to manage privileged access is to be used across the ITS organization.

Principle 2: All privileged access management activities must be appropriately documented within the ITSM toolset.

Principle 3: Authorization and attestation of privileged access is the responsibility of the system and/or ITS service owner.

Principle 4: Approvals and authorizations for privileged accounts must not be delegated.

Principle 5: Privileged access to systems is granted on a least-privilege basis.

Principle 6: Privileged access account passwords are in compliance with the corporate password standard, subject to any system limitations.

Principle 7: System and service owners perform a quality review and assessment of privileged access as part of their role responsibilities.

4. ROLES AND RESPONSIBILITIES

4.1.Local Regional Authorities and SWODIN Service Owners

- Approve creation of, modifications to, or the disabling / removal of privileged access accounts
- Ensure only authorized individuals can create system administrator or privileged access accounts
- Ensure privileged access accounts are designed with least-privileged access possible and consider potential segregation of duty conflicts
- Ensure access to privileged access accounts is limited to appropriate personnel
- Annual report to review privileged access accounts and attestation
- Review eHealth's policies for any recommendations to implement for the DI-r systems on an annual basis.
- That upon role change, department change, resignation or termination, that the assigned privileged access account is disabled, or password reset, within one-business day

4.2.System Administrators

- To ensure requests for privileged access accounts have been documented and requested in accordance with the standard and process documents
- To ensure the appropriate approval is in place before adding, modifying or removing/disabling a privileged access account
- Privileged access accounts are created with least-privilege access possible
- Assist Local Regional Authorities to pull and document privileged user reports
- Make post-attestation modifications to privileged access accounts, based on Local Regional Authorities reviews
- Monitor privileged access accounts for abuse or inappropriate activity

4.3.Privileged Users

- Privileged access accounts are used only when that level of access is required to perform authorized tasks
- Existing default service account passwords are changed when setting up new systems
- Document assignment, requirements and description of privileged access accounts
- Review user activity reports, for their local site, for regular review and attestation
- Only use this access to perform their assigned job duties
- Not access or attempt to access information above and beyond what is required by their job duties or contracted services, even if the system allows them to do so

5. PROCESS

There are four processes involved in managing privileged access:

1. Requesting / modifying access – A request must be submitted and approved by a Local Regional Authorities and then sent to the SWODIN system administrator for processing and documentation.
2. Terminating access – A request must be approved by a Local Regional Authority, and follow the local hospital policies and standards for account suspension. Requests are also submitted to the SWODIN system administrator for processing and documentation.
3. Attestation – Local Regional Authorities are to review privileged access accounts, annually, to ensure all privileged access, at the local site, is appropriate based on the users job responsibilities and that the level of access does not create a segregation of duties concern. The final attestation is then signed and submitted to the system administrator for processing (making any required updates per the Local Regional Authority's review) and documentation.
4. Monitoring privileged access – Local Regional Authorities will be responsible to ensure the appropriate mechanisms are in place to review and identify privileged level activity, such as access logs. Where feasible privileged level activity will be reviewed and accessed for appropriateness.

5.1.Process Roles and Responsibilities RACI

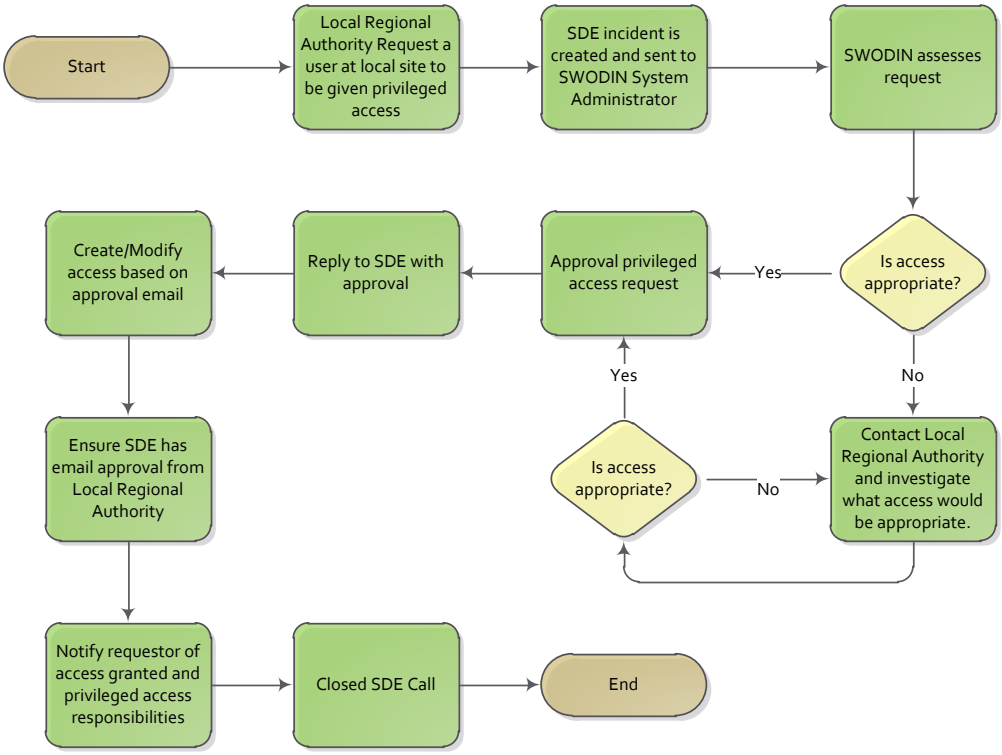
Process Activity	SWODIN	Local Regional Authority	Privileged User
Requesting new, modifications to, disabling or removal of privileged access accounts	R	A,R	I, R
Approving new, modifications to, disabling or removal of privileged access accounts	R	A	R
Creating, modifying, disabling/deleting privileged access accounts	R	A	R
Pulling and providing lists to system owners for attestation	A	R	R
Review and Attestation of privileged access accounts	R	A	R
Post-attestation modifications and documentation	R	A	I
Monitoring of privileged access accounts	R	A	R
Record and store review and attestation results system owner	A,R	I	-
Record and store review and attestation results ITS	A,R	I	-

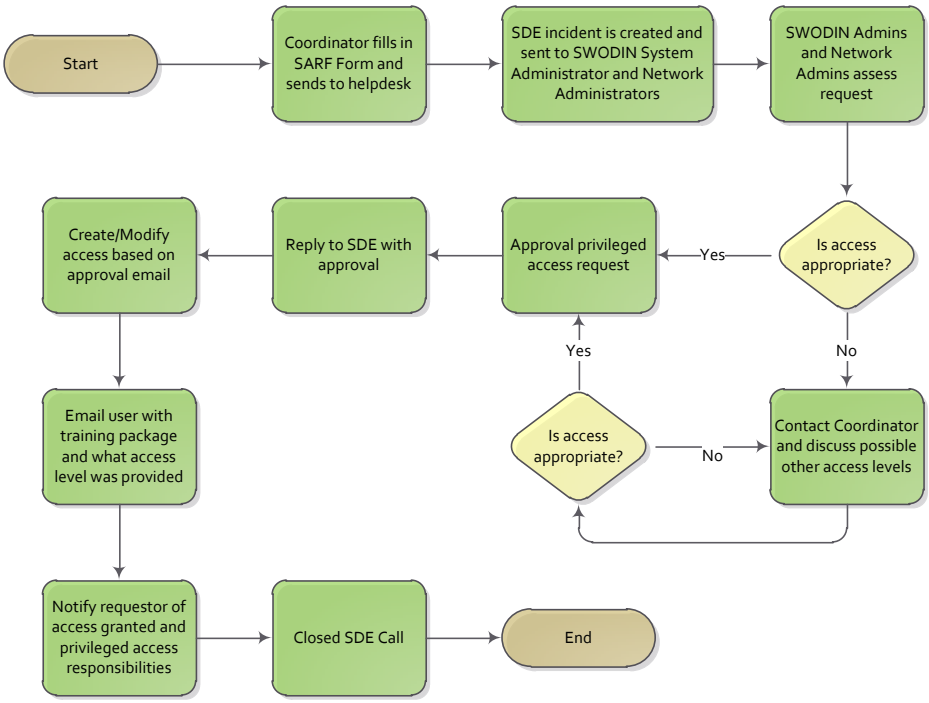
DEFINITIONS

A: ACCOUNTABLE *- The accountable person is the individual who is ultimately answerable for the activity or decision. This includes "yes" or "no" authority and veto power. Only one "A" can be assigned to an action.*

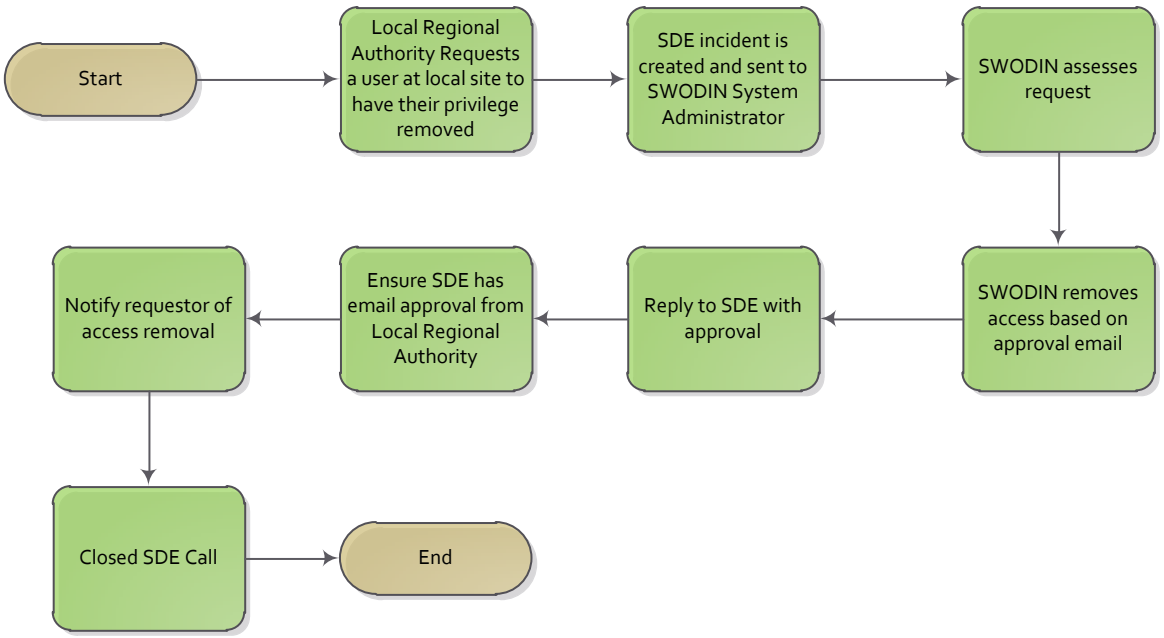
R: RESPONSIBLE – *The "doer." This is the individual(s) who actually complete the task. The "doer" Is responsible for action/implementation. Responsibility can be shared. The degree of responsibility is determined by the individual with the "A".*
C: CONSULTED - *The consulted role is the individual(s) (typically subject matter experts) to be consulted prior to a final decision or action.*
I: INFORMED - *This is the individual(s) who needs to be informed after a decision or action is taken. They may be required to take action as a result of the outcome.*

5.2.Granting and Modifying Access

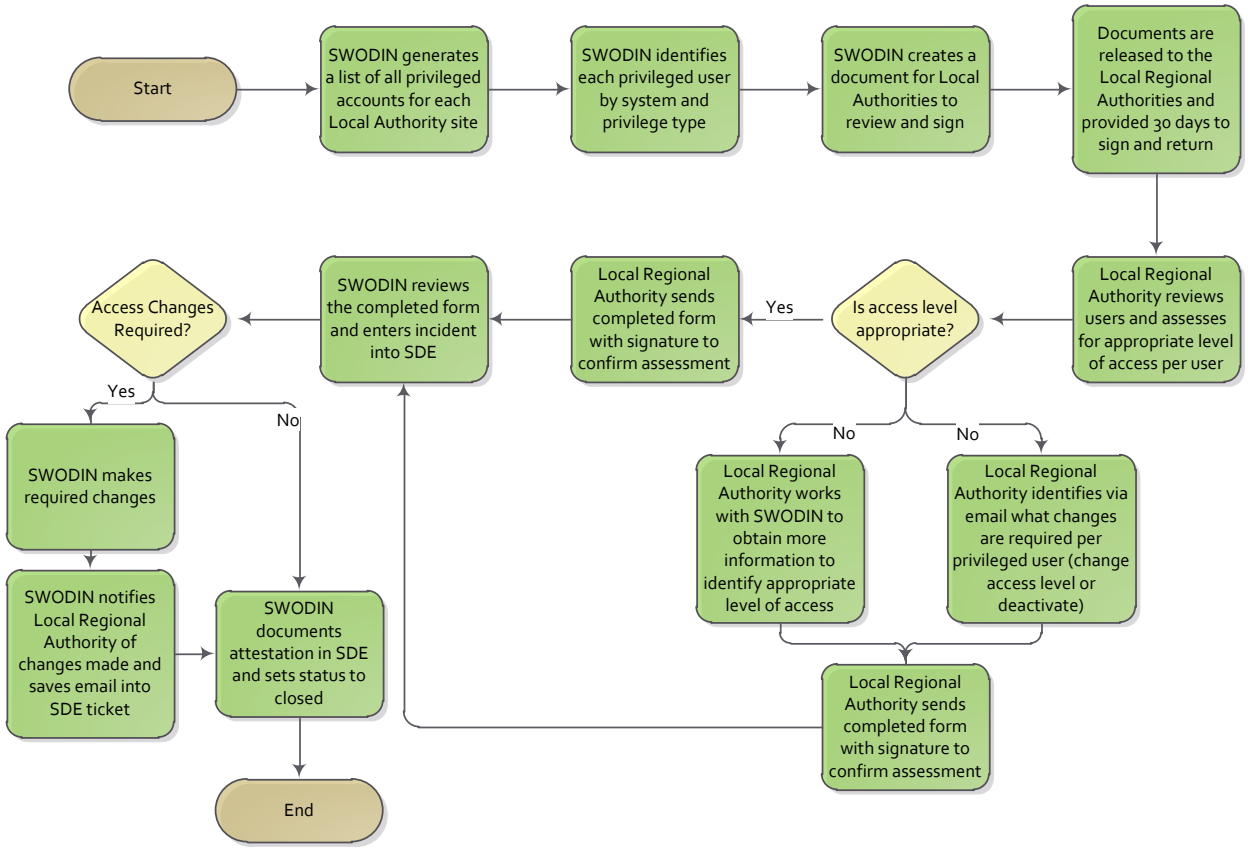




5.3.Terminating Access



5.4.Attestation



6. Definitions

ITS Service Owners - are ITS Management representatives who are accountable for service delivery, service quality and customer satisfaction.

ITS Management Representatives - Manager PACS/DI-r - PACS and DI-r systems

Least Privilege – When creating an end-user or privileged account, one is to ensure that only the privileges that are required are assigned which are commensurate with that individuals role responsibilities.

Privileged Access – Access privileges greater than those of a standard user account, typically used to perform administrative duties within a system. Privileged access could include the ability to perform:

- System configuration changes
- System updates/patches
- User account creation
- Password resets
- Modifications to account privileges
- Modifications to data and table structure through the back-end (database)
- Modifications to system files at the operating system and server level

Segregation of Duties – Also known as Separation of Duties, is the idea of more than one individual performing a task intended to prevent error or fraud. An example of this would be a developer create coding for a production environment, but requiring another individual to promote that code into production.

System Owner/SWODIN Coordinator: Is the clinical or business person, whether corporate or departmental, with the authority to make the day-to-day decisions for a system, such as approving updates, or the addition or removal of user accounts. A system includes all of the layers that it comprises: the application, the database, the server, and the infrastructure to connect to it.

Local Regional Authorities: Is the clinical or business person, at a partnered hospital or independent health facility, whether corporate or departmental, with the authority to send information from the local site to the DI-r system, use the DI-r system and approving addition or removal of user accounts.

System - A system includes all of the layers that comprise it: the application, the database, the operating system and the server or servers they are installed on.

System Administrator: One whose role is to perform activities which may affect applications and / or systems, servers, network communications, end-user accounts, files, data, or processes of users. These activities may include, server builds, installing software, patching or updating systems, backing up systems, securing systems, auditing systems, enabling, disabling or applying resources to end-user accounts, creating privileged or system administrator accounts, monitoring and repairing systems. This definition could include those with roles or job titles such as: Technical support staff, database administrators, network administrators, technical analyst, support analyst, vendor or consultant.

Document Revision History

Revision	Author	Date	Comments
1.0	Arielle Fuller	Aug 17, 2016	Original draft