RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Rutgers Provisioning/Deprovisioning Policy				
Section #:	70.1.7	**Section Title:**	Information Technology: Information Technology Policies	**Formerly Book:**	N/A
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer	**Adopted:**	04/23/2021	**Reviewed:**	
Responsible Executive:	Senior Vice President and Chief Information Officer	**Revised:**			
Responsible Office:	Office of Information Technology (OIT)	**Contact:**	oit-policies@oit.rutgers.edu		

1. Policy Statement

This document outlines the rules, regulations, and procedures for provisioning and deprovisioning accounts and access rights on Rutgers, The State University of New Jersey, systems.

2. Reason for Policy

Having a standard provisioning and deprovisioning policy for accounts and access rights for the entire University allows for the adherence to federal, State and local, legal, regulatory, and statutory requirements, as well as minimizes University risk for unauthorized access to University systems, information, and facilities.

3. Who Should Read This Policy

All members of the Rutgers University community.

4. Resources

University Policies: Information Technology - Section 70

University Policy 30.1.8: Access to University Facilities

University Policies: Human Resources (HR) – Section 60

University Policy 70.1.1: Acceptable Use Policy for Information Technology Resources

University Policy 70.1.2: Information Classification

University Policy 70.1.6: Email and Calendar Policy

University Policies: Clinical, Compliance, Ethics & Corporate Integrity - Section 100

Office of Information Technology (OIT) Help Desk: https://oit.rutgers.edu/help

Office of Information Technology (OIT) Policies Website: https://oit.rutgers.edu/policies

NetID Activation Website: https://netid.rutgers.edu/

Email and Calendar Website for Rutgers Connect: https://oit.rutgers.edu/connect

Email and Calendar Website for ScarletApps: https://oit.rutgers.edu/scarletapps

5. Definitions

Access Rights - The permissions granted to a user to read, write, or erase files in information systems.

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization - The process of verifying that a requested action or service is approved for a specific entity.

Deprovisioning - The process of removing access rights of all employees and external parties to information and information processing facilities upon termination of, or change to, their employment, contract, or agreement.

Information Owner - An organizational official with statutory, management, or operational authority for specified information who is responsible for establishing the procedures governing its generation, collection, processing, dissemination, and disposal. [National Institute of Standards and Technology Special Publication 800-12]

Privileged Accounts - A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. National Institute of Standards and Technology Special Publication Computer Security Resource Center (NIST)

Procedures - Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

Provisioning - Defines the accounts and access rights that are authorized to users or automatically granted for users by the user's role.

System Owner - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

System Account / System Service Account - A user account created by an operating system and used for the operating system's defined purposes. Some, for example *root*, may also be logged into by system administrators.

Technology standards - Established requirement of technical configuration parameters and associated values to ensure that management can secure University assets and comply with University policy and regulatory requirements. It is a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices.

University Business - Work performed as part of an employee's job responsibilities, daily work, and duties performed on behalf of the University by faculty, staff, student workers, guests, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. This includes any email, calendar events, files, or other electronic business data, created, stored, processed, and transmitted that is related to work performed for Rutgers.

User - An individual, group, or organization granted access to organizational information in order to perform assigned duties. [National Institute of Standards and Technology Special Publication 800-12]

User Account - The collection of specific access privileges for authorized users to gain access to information systems.

6. The Policy

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of University information collected, processed, stored, or transmitted in accordance with the standards outlined in this Policy.

A. Responsibilities:

Executive/Senior/Vice Presidents, and Chancellors:

- Are responsible for safeguarding their organization's electronic information and information systems.
- Must ensure that each member of their organization understands the need to protect the University's electronic information and information systems.
- Must communicate this policy to all members of their organization.
- Must establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

Deans, Directors, and Department Chairs:

- Are responsible for safeguarding the electronic information and information systems of each business unit in their area of oversight.
- Must ensure that the members of each business unit in their area of oversight understands the need to protect the University's electronic information and information systems.
- Must communicate this policy to all members of each business unit in their area of oversight.
- Must establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.
- Must ensure that when the status of an employee within their organization changes (transferred, terminated, or otherwise separated) the appropriate deprovisioning procedure is followed to notify the system owners of the change in authorization to systems for which the employee had previously authorized access.

Information or System Owner Responsibilities, **include but are not limited to:**

Provisioning:

- Establish access control rules appropriate for the classification of information within the system and types of users who will be accessing the system, access rights, and restrictions for specific user roles toward their assets, with the amount of detail and the strictness of the controls incorporating separation of duties.
- Establish and document appropriate logical and physical access controls.
- Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

- Provide users and service providers a clear statement of the business requirements to be met by access controls.
- Establish formal access authorization procedures to their electronic information and information systems.
- Maintain an inventory of requests for access with pertinent information such as user ID, contact information, etc.
- For electronic protected health information (ePHI) information systems, establish procedures for obtaining necessary electronic protected health information during an emergency as required by HIPAA § 164.312(a)(2)(ii).
- Perform and comply with the policy requirements relevant to their information systems.
- Review access entitlements to their information systems as stipulated in this Policy or when requested by the Office of Information Technology (OIT), and/or Audit and Advisory Services.

Deprovisioning:

- Review Daily Report and requests from Business Units/Schools for those transferred, terminated, or otherwise separated from the University and ensure the access rights to information and assets associated with information processing facilities and services are removed or suspended.
- Upon notification from Deans, Directors, or Department Chairs, remove access as requested for employees who have changed status within each business unit in their area of oversight.
- Changes of a user's employment, contract, or agreement should initiate the removal of all access rights that were not approved for the new employment.
- Access rights removed or adjusted should include those of physical and logical access. Removal or adjustment can be done by removal, revocation, or replacement of keys, identification cards, information processing facilities, or subscriptions.
- Documentation that identifies access rights of employees and contractors should include a record of the removal or adjustment of access rights.
- If a departing employee or external party user knows passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract, or agreement.
- Have access rights of employees and external parties to information and information processing facilities reduced or removed before the employment terminates or changes, depending on the evaluation of risk.
- Have the access rights of all employees and external party users to information and information processing facilities removed upon termination of their employment, contract, or agreement, or adjusted upon change.

The User Responsibilities, include but are not limited to:

- Adhere to all policies that govern acceptable use of organizational systems;
- Use the organization-provided IT resources for defined purposes only; and
- Report anomalies or suspicious system behavior. [National Institute of Standards and Technology Special Publication 800-12]

B. Requirements:

1. Access Controls:

Registration of Access

- Access must be granted on the basis of least privilege and only to resources required by the current role and responsibilities of the person. In addition to the administrative, physical, and technical safeguards presented in this Policy, the security requirements outlined in University Policy 70.1.2: Information Classification must be adhered to.
- Access to all University information systems must have an authorized, formalized, and approved documented process by the Information or System Owner or delegate.

Registration of Access for Non-Rutgers Personnel

- Individuals who are not members of the Rutgers community and who have a justifiable business reason to gain access to Rutgers information services must go through the guest account registration process, including the Registration of Access.

Information System Identity Access Management

Information systems must, at minimum, require a user ID (e.g. an individual digital identifier called a “NetID”) and password.

Passwords

- Passwords must be configured to follow OIT standards and/or vendors’ recommendations for strong passwords.

Generic User Accounts

- Generic User accounts are subject to the requirements in this policy and must be restricted to kiosks or specialty devices where standard authentication may impede the functionality of the device.

Guest Accounts

- Guest accounts are subject to the requirements in this policy and have a lifecycle no longer than 18 months, after which they must be re-approved by the sponsor.
- The accounts and associated access rights must be sponsored by a Rutgers employee who is responsible for the safeguarding of the information or information system as detailed in the Section – Separation of Duties.

Service Accounts on Rutgers Active Directory (RAD) and in Rutgers Identity Management (IDM) components

- Service account creation is restricted to authorized administrators and provided only upon an identified operational need.
- Service accounts can only be created by a member of Rutgers’ Active Directory or Domain Administrators teams or by authorized members of Identity and Access Management Organizations to facilitate an identified operational need.
- Service accounts do not expire.

System Service Accounts

- Whenever possible, system default service accounts should be renamed and disabled as long as it does not adversely impact the operations of the application or other dependencies.
- System default Service Accounts do not expire.

Privilege Accounts

- Authorizations for privileged access rights should be reviewed at least every six (6) months.
- Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained.
- Changes to privileged accounts should be logged for periodic review

System and application access control

- Access to information and application system functions should be restricted in accordance with this Policy.
- Restrictions to access should be based on individual business application requirements.

Emergency Access to electronic protected health information (ePHI) Information Systems

- Emergency access procedures must have the ability to access ePHI during a health emergency.
- Emergency access procedures must have a contingency method to access ePHI if a natural or man-made disaster makes an information system unavailable.
- Any deviation from these requirements must be documented and approved by delegates from University Ethics and Compliance and the Office of the Senior Vice President and General Counsel.

Facility Access

- Security perimeters should be defined and used to protect areas that contain either *Critical* or *Restricted* information, as defined by the University Policy 70.1.2: Information Classification, or are the University's information processing facilities.
- Physical access to the facilities where information systems are housed must be limited to personnel specifically approved by the data center manager.
- Access rights to secure areas should be regularly reviewed and updated and revoked when necessary.

2. Separation of Duties

- Access requests, authorization, and administrative responsibilities for information classified as *Critical* or *Restricted* (otherwise considered sensitive), as defined by the University Policy 70.1.2: Information Classification, and their associated information systems should be separated.
- Users should not have access privileges that would permit them to approve their own changes to an information system or electronic record.
- If separation of duties is not possible due to staffing limitations, other mitigating controls must be in place to reduce the risk of fraud or tampering.

3. Transfers within the University

- Access requests, authorization, and administrative responsibilities for information classified as *Critical* or *Restricted* (otherwise considered sensitive), as defined by the University Policy 70.1.2: Information Classification, and their associated information systems should be removed.
- If the employee requires some of the data from his/her Rutgers Connect account as part of the transfer to the new department, the following process must be adhered to:
  - Faculty/staff submits written request to department head of exiting department.
  - Department head of exiting department needs to approve and sign off on this data transfer within 15 days.

- If data involves Protected Health Information (PHI), the Health Insurance Portability and Accountability Act (HIPAA) University Ethics & Compliance Privacy Director needs to approve and sign off as well.
- If approved, the delegated administrators from the exiting department and the new department will work with the employee to migrate the account from the existing location to the new location, along with the appropriate data in the account. Any data deemed inappropriate would not be migrated.

4. Access Entitlement Review

- Access rights to information systems with data classified as *Critical* or *Restricted,* as defined by University Policy 70.1.2: Information Classification, must be reviewed at a regular, formalized, documented interval.

5. NetIDs, Email Accounts and Access Rights

NetID's, email accounts, and access rights will be provisioned and deprovisioned as outlined:

Provisioning:

- Source system for Rutgers affiliates to be provisioned a NetID include:
  - Human Resources for Faculty, Staff, and Retirees
  - Student systems for Students and Alumni
  - Guest system for Other Affiliates
- Once provisioned, the Rutgers affiliate is required to activate their NetID prior to use.
- If an individual with a previous affiliation returns to Rutgers, they will be reassigned the same NetID.
- Every Rutgers affiliate who has an active NetID is eligible for an account on one of the approved email and calendaring systems.
- Alumni who choose to maintain a Rutgers email account will be provisioned (or continue to keep their previous) ScarletMail account.
- Retirees who choose to maintain a Rutgers email account are entitled to an account on ScarletMail upon retirement or to request the provisioning of a new ScarletMail account. Their previous Rutgers Connect account will be inactivated.
  (Note: Emeritus Faculty who retire have the option to retain their Rutgers Connect account or transition to a new email account on ScarletMail.)

Deprovisioning:

- When a Rutgers affiliate no longer has an active role at the University, based on notification from source systems, their NetID, used for authentication, is immediately inactivated.
- In the event a NetID needs to be inactivated immediately, the manager/supervisor shall limit or cancel access to computer accounts by contacting the OIT Help Desk to deactivate the NetID.
- Faculty, staff, and students who no longer have an affiliation with Rutgers are no longer eligible to have a Rutgers email account. The email account and its access rights are inactivated upon notification from source systems.
- Faculty and Staff who retire from the University are eligible to maintain a Rutgers email account, however this will not be the Rutgers Connect account previously utilized for University business. A new email account and access rights for the retiree will be provisioned on ScarletMail. (Note: Emeritus Faculty who retire have the

option to retain their Rutgers Connect account or transition to a new email account on ScarletMail.)

- Faculty and Staff who have been laid off from Rutgers but have recall rights can choose to maintain a Rutgers email account, which will be provisioned on ScarletMail during the recall rights period.
- In the circumstance where a faculty/staff Rutgers account is inactivated, and a department or third party request access to data contained within the inactivated account for Rutgers business continuity or for reasons other than business continuity, the request should be submitted to the Office of Ethics and Compliance for approval before the Rutgers delegated administrators responsible for the department or the Messaging Group will release the data to the requesting party. When Faculty or Staff transfer within Rutgers, from one department to another, the department head of the exiting department may decide that the nature of a departing Faculty or Staff's data is of such a confidential nature that all the data must be removed from the Rutgers Connect account prior to the delegated administrator releasing the account to the new location. In this case, if the employee would like to retain some of the data from his/her Rutgers Connect account as part of the transfer to the new department, the following process must be adhered to:

    - Faculty/staff submits written request to department head of the exiting department.
    - Department head of exiting department needs to approve and sign off on this data transfer within 15 days.
    - If data involves Protected Health Information (PHI), the Health Insurance Portability and Accountability Act (HIPAA) University Ethics & Compliance Privacy Director needs to approve and sign off as well.
    - If approved, the delegated administrators from the exiting department and the new department will work with the employee to migrate the account from the existing location to the new location, along with the appropriate data in the account. Any data deemed inappropriate would not be migrated.

- When an employee has a dual assignment, where the Rutgers Connect account is with the primary assignment's domain, and his/her primary assignment ends, the department head of the old prime department may decide that the nature of the employee's data is of such a confidential nature that all the data must be removed from his/her Rutgers Connect account prior to the delegated administrator releasing the account to the new primary assignment location. In this case, if the employee would like to retain some of the data from his/her Rutgers Connect account as part of the transfer to the new department, the following process must be adhered to:

    - Faculty/staff submits request to primary assignment department head.
    - Department head of primary department needs to approve and sign off on this data transfer within 15 days.
    - If data involves Protected Health Information (PHI), the HIPAA University Ethics & Compliance Privacy Director needs to approve and sign off as well.
    - If approved, the delegated administrators from the exiting department and the new department would work with the employee to migrate the account from the existing location to the new location, along with the appropriate data in the account. Any data deemed inappropriate would not be migrated.

7. Non-Compliance and Sanctions

Failure to comply with this Policy may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable State and federal statutes.