RIT Information Security

Account Management Checklist

Account name: ____

Completed by (please print): ________________________ Date: _______________

Signature: ___________________________ Next scheduled review date: _______________

Manager’s signature: ___________________________ Date: _______________

Account Authentication	*Ref.*	**Initials**
1. End user account authentication uses the enterprise identity and access management service when the system or application processes Private, Confidential, or Critical Process information.	*(1.1)*	
2. The use of the enterprise authentication service by an application is authorized by the Authentication Service Provider and the security review by the Information Security Office.	*(1.2)*	
3. Access to passwords and their hashes is restricted.	*(1.3.1)*	
4. Public terminals and kiosks do not cache user passwords/passphrases.	*(1.3.1)*	
5. All password changes are logged, but the password itself is not logged.	*(1.3.2)*	

Account Authorization	*Ref.*	**Initials**
6. Account authorization uses central identity and access management services when system or application processes Private/Confidential or Critical Process information.	*(2.1)*	
7. Data owner has authorized: □ A process for approving and documenting authorization. Authorization granted to an account should be commensurate with the level of identity validation performed. □ The parties who may approve user access to roles. □ Roles and their privileges following the security principles of Least Required Access and Segregation of Duties.	*(2.2)*	

Account Provisioning	*Ref.*	**Initials**
8. The account is for individual use with an academic or business need for this access.	*(3.1)*	
9. Employees with multiple roles with the University have role-based access or – if this cannot be achieved technically – separate accounts are used for each role.	*(3.1.1)*	
10. Student employees have separate accounts from their student accounts.	*(3.1.2)*	
11. Student accounts do not have student employee-related access?	*(3.1.2)*	
12. Physical access grated by student IDs has a pre-populated termination date.	*(3.1.3)*	
13. Accounts are valid when the individual account holder has authorized access to the account or until the account is suspended by the University.	*(3.2)*	
14. Authorized Administrators: □ Review approvals and provision account/access. □ Track authorizations, including date of authorization, identification of individual approving access, and identification of the role assigned or description of the access privileges granted. □ Grant access privileges only to be used to fulfill assigned job duties. □ Retain authorizations in accordance with the Records Management Policy (C22.0).	*(3.3)*	

Account Management and Maintenance	Ref.	Initials
15. Managers review account and access privileges with employees upon notification of job changes (e.g., termination, job changes).	(4.1.1)	
16. Data owners of private information review accounts and access privileges annually (at minimum) to ensure that they are commensurate with job function, need-to-know, and employment status. Date of last review: _______	(4.1.2)	
17. Managers communicate to account administrators when an account or access privileges may require modification or deactivation.	(4.2)	
18. Upon notification, the account administrators review account and access privileges modifications with the data owner or designee. Changes are formally documented.	(4.3)	
19. Upon notification, accounts immediately deactivate and access privileges are removed when continued access is no longer required (e.g., terminated). Deactivation is formally documented.	(4.4)	
20. Authentication systems disable user accounts after a set number of logon attempts.	(4.5.1)	
21. Owners follow established procedures for re-enabling/-setting user accounts using proper verification of user identity (do not use UID as the sole verification method)	(4.5.2, 4.5.3)	

Additional Requirements for Provisioning Administrator and Service Accounts	Ref.	Initials
22. Administrator accounts or groups are assigned to a single individual. Service accounts are assigned to a system or application - NOT an individual.	(5.1.1) (5.1.2)	
23. Administrator and Service Accounts are specifically for system or application use only.	(5.2)	
24. Administrator and Service Accounts are shared by a limited group of individuals for the purpose of operation and administration of the application or system, and only where required by the system or application. (In these cases, when possible, access to system accounts is by a method that allows the individual to authenticate using a username and password.)	(5.3)	
25. Have you removed, disabled or changed (in that order) any default accounts (configuration access, database accounts, etc.)?	(5.4)	
26. Confirm that if an account administrator is no longer in that role, related service accounts were reassigned and passwords of the service accounts changed.	(5.5)	

Additional Requirements for Sponsored Accounts	Ref.	Initials
27. Only authorized RIT account holders can approve sponsored accounts.	(6.1)	
28. Sponsored accounts have an expiration date of no more than one year or the work completion date, whichever occurs first.	(6.1)	
29. Upon termination of the Sponsor's account, the Sponsored account is transferred to another appropriate RIT account holder or deactivated.	(6.2)	

Additional Requirements Shared & Generic Accounts	Ref.	Initials
30. Shared/generic account has one designated owner. The owner should log access to the generic or shared account.	(7.1)	
31. Generic accounts may only be shared in those situations where a system (server), device (switches or routers) or application cannot support the use of individual accounts technically.	(7.2)	

After completing this checklist, please keep a copy with your account management documentation and make it available to the RIT Information Security Office on request.

For more information, contact:
RIT Information Security
585-475-4122
infosec@rit.edu
https://www.rit.edu/security