**Assignment 4-3 Activity:**

**Role-Based Access Control (RBAC) Matrix**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

March 31, 2024

# CYB 200 Module Four Activity Template

After reviewing the scenario in the Module Four Activity Guidelines and Rubric document, fill in each cell with one or more of the following actions:

* View
* Create
* Modify
* Delete
* None

| **User name** | **Patient information** | **Employee information** | **Access to the SaaS** | **Access to backup logs** |
| --- | --- | --- | --- | --- |
| Norman | None | View, create | View, create, modify | View |
| Ryhead | View | None | View, create | None |
| Simone | None | View | View | None |
| Janet | None | None | View, create, modify, delete | View, modify, delete |
| Dale | View, create, modify | None | None | None |
| Ethan | View | None | None | View |

After you have completed the table above, respond to the following short questions:

* 1. What changes could be made to user roles through implementation of least privilege to better support that security design principle? (Hint: Refer to the characteristics in the *user job roles and characteristics* table in the scenario, and consider the characteristics that may be contradictory.)
* By implementing the security design principle of least privilege, we can ensure that each user role has only the necessary permissions to perform their specific job functions while minimizing access to sensitive data and software access. Least privilege is the “principle in which a subject should be given the minimum level of rights necessary to perform legitimate functions” (Kim & Solomon, 2023, p. 512). This will allow individuals to perform their job duties successfully without potential unauthorized access to information and software. A change to implement least privilege would be to remove the ability for Norman to create user accounts and assign passwords. Since Norman is a remote call center employee, he should not have access to create user accounts and assign passwords. Also, taking away this access would not affect Norman’s ability to perform his job duties as a call center employee. Another change that can be made is to limit Simone’s access to employee information only. Since Simone is an HR representative, they do not need access to patient information, software, or backup logs. These changes will help align user roles more closely with the principle of least privilege, which will reduce the risk of unauthorized access or security breaches while still allowing users to perform their primary job functions.
  1. What is the importance of this tool to you as a security analyst in managing and protecting the environment? Provide an example.
* As a security analyst, a Role-Based Access Control (RBAC) matrix is an important tool for managing and protecting the environment. The benefit of using RBAC as a security analyst is “its ability to represent the structure of the organization and force compliance with control policies throughout it” (Kim & Solomon, 2023, p. 196). Implementing RBAC in a logistical environment will help a security analyst manage the basic roles of supply chain managers, accounts receivable and accounts payable, human resources (HR), and forklift operator, allowing proper access to information and systems. For example, a supply chain manager will need access to specific software, such as enterprise resource planning (ERP), to manage inventory and the purchasing of products. As for a human resources employee, they have their own software that allows them to access employee information and don’t need access to ERP systems to perform their job functions as HR. Allowing a supply chain manager access to HR software or applications can lead to a potential security breach or accidental leak of sensitive information since supply chain managers are not specifically trained to understand HR systems. This also applies for other roles having access to systems or software outside of their specific job roles. Using RBAC as a tool will help the security analyst understand and manage permissions to each job function and systems within the logistical environment creating structure, security, and compliance in the organization.

**Reference**

Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. <https://openpage-ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST> 3209c3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1