

## Information Security Office (/)

Home (/home) » Separation of System Resources Guideline

# Separation of System Resources Guideline

**NOTE: The Information Security Office recently updated the UC Berkeley's Data Classification Standard and Protection Profiles for the Campus. These number changes are reflected on this page.**

*UC Berkeley security policy mandates compliance with Minimum Security Standard for Electronic Information (<https://security.berkeley.edu/mssei>) for devices handling covered data. The recommendations below are provided as optional guidance for separation of system resources (<https://security.berkeley.edu/mssei-controls#separation>) requirements.*

## Requirement

Resource Proprietors and Resource Custodians must appropriately limit the sharing or re-use of application credentials, service accounts, user accounts, databases, and system hardware across unique systems or environments.

## Description of Risk

Sharing between systems or services increases security risk. A compromise of one system can lead to a compromise of all of systems sharing the same database or credentials.

## Recommendations

### Separate Application Credentials

Shared application credentials are user accounts where passwords are known to multiple individuals, allowing these individuals to login using the same account information. The risk is that when credentials are shared, system changes and activities are linked to the shared user account, but not the individuals using the account. Thus it becomes difficult to trace problem sources and assign accountability in cases where errors or malicious activities occur. It also increases the likelihood of compromise since compromise to any one of the individuals sharing the account credential will also likely lead to compromise of the shared account.

1. Resource Proprietors and Resource Custodians should create one application account per individual, so that there is no sharing of an individual account between multiple people. The use of shared accounts should only be permitted where necessary for business or operational reasons and should be approved and documented by resource proprietors.
2. Application users, including administrators, should use unique credentials linked to their personal identity so all activities can be traced to their source.
3. Individuals in possession of credentials with access to covered systems must utilize a passphrase that are significantly different for each separate account under their control. "Significantly different" means passphrase permutations should not be based on commonly used patterns (<http://www.microsoft.com/security/online-privacy/passwords-create.aspx>) since modern password cracking software has built-in algorithms to check for these patterns.
4. Develop a process to manage and monitor application users accounts based on MSSEI Account Monitoring and Management requirements (<https://security.berkeley.edu/mssei#account>).
5. All administrative accounts must be protected by complying with MSSEI Controlled Use of Administrative Privileges requirements (<https://security.berkeley.edu/mssei#admin>).

## Separate System Resources

Critical services storing, processing and transmitting covered data should be hosted on separate physical or logical servers to reduce the risk of a compromised service negatively impacting other services hosted on the same server. Consider the following recommendations when designing system architecture to properly separate system resources:

1. Operate critical services, such as file, mail, web, and database servers, on separate physical or logical host machines.
2. Limit the sharing of resources (storage, network and computing) between applications and data from different classification levels. For example, the same physical server or VM (virtual machine) server should not be used to run a database that stores both UC P4 and UC P1 data. Instead, UC P4 data should be moved to a separate server (physical or VM) that complies with MSSEI requirements.
3. Ensure that network traffic of covered data between physical or logical host machines adheres to encryption in transit requirements (<https://security.berkeley.edu/mssei#dlp>).
4. Covered data and critical services should operate on host devices that are logically or physically separated on the network from devices hosting non-covered data and services as directed by MSSEI Boundary Defense requirements (<https://security.berkeley.edu/mssei#boundary>).

Note that when a device (server) stores, processes and transmits varying protection levels of data, unless the data is segregated per recommendation #2, the device must comply with the highest level of security requirements. For example, a device that stores UC P2/P3 and UC P4 data must adhere to security standards applicable for UC P4 covered devices.

## On This Page

- Requirement
- [Description of Risk](#)
- [Recommendations](#)

Powered by Open Berkeley (<https://open.berkeley.edu>)

Accessibility (<https://dap.berkeley.edu/get-help/report-web-accessibility-issue>)

Nondiscrimination (<https://ophd.berkeley.edu/policies-and-procedures/nondiscrimination-policy-statement>)

Privacy (</website-privacy-statement-berkeley-security>)

Copyright © 2024 UC Regents; all rights reserved

[Back to Top](#)