

CCS Administrative Procedure

8.10.01–D Shared Accounts

Implementing Board Policy [8.10.01](#)

Contact: Chief Information Officer, 533-8833

1.0 Purpose

The purpose of this procedure is to help ensure the security of Spokane Colleges information technology systems by establishing guidelines and expectations for the use of shared accounts and logon IDs while ensuring compliance with the standards, policies, and guidelines of Washington Technology Solutions (WATech).

2.0 Limitations and Requirements

Spokane Colleges recognizes the importance of information security, that accounts shared or used by more than one (1) user of a given information technology asset or resource obscure identity and therefore accountability, and that the WATech standards, policies, and guidelines prohibit the use of group, shared or generic logon IDs and passwords.

- 2.1 This procedure applies to accounts used by employees, students and third-party entities at Spokane Colleges. This procedure applies to all equipment that is owned or leased by Spokane Colleges and to all internet-based (cloud) services authorized and subscribed to by Spokane Colleges.
- 2.2 This procedure assumes ALL employees and ALL students have a ctcLink ID number and a unique CCS network login account to be used to comply with this procedure.
- 2.3 This procedure establishes an expectation and guideline to reduce or eliminate the use of shared logon IDs to control IT network, data and resource access, and to facilitate better audit trails and incident responses for network breaches or other violations of acceptable use.

3.0 Standards and Guidelines

- 3.1 When user login accounts are available, those accounts will be used to login to Spokane Colleges computers/devices and information technology services.
- 3.2 When a student or employee does not have a user login account, one will be created for them as a standard Information Technology security business practice.
- 3.3 The use of shared logon IDs is prohibited, except when authorized and approved by the Director of Technology Services or the Information Security Officer. Any requests for an exception shall be furnished in writing no fewer than 10 business days prior to the date the exception must take effect. Some example cases are described below:
 - 3.3.1 When a class or event is being conducted by the colleges or district office where the use of a computer is required, and there are no student or employee accounts available for the participants to use, it may be permissible to use a shared account. Note that any such account will likely be limited to allow logins only on specific computers/devices.
 - 3.3.2 When approved software is being used that cannot work with individual accounts due to licensing or technical constraints, it may be permissible to use a shared account. Note that any such account will likely be limited to allow logins only on specific computers/devices.
 - 3.3.3 When there is a demonstrated requirement for functionality, it may be permissible to use a shared account. Note that any such account will likely be limited, tracked, and audited to allow logins only on specific computers/devices.

4.0 Related Information

- 4.1 [CCS Administrative Procedure 8.10.01-A](#) – Acceptable Use of Information Technology
- 4.2 [CCS Administrative Procedure 8.10.02-A](#) – IT Security
- 4.3 [WATech Standard SEC-0](#) – Securing Information Technology Assets

Originated: April 2025
Cabinet approval: May 2025