



SECURED DOCUMENT

Approval Date: MM/DD/YY

Effective Date: MM/DD/YY

## ADMINISTRATIVE RULE

Last Revised: 03/06/2020

---

<b>Rule Number/Name:</b>	080.013.000- System and Data Backup Provisions
<b>Responsible Department:</b>	Information Technology Services
<b>Authority:</b>	Chief Technology Officer

### Overview

*This document should be considered a security document and NOT publicly distributed.*

This document summarizes the fundamental structure of our System Data Backup provisioning.

These rules are in place to provide a structure to optimize business continuity.

This document also summarizes the basic process structure used for recovery.

### Applicability

These rules affect how Columbia Gorge Community College's (CGCC's) Information Technology Services (ITS) Department manages data and system backups.

Not following these rules places the College business continuity at risk.

### Administrative Rule Statement

CGCC's ITS Department strives to follow industry standards for redundancy and backup methods. It is our responsibility to provide the necessary provisions needed for backups, disaster recovery and contingencies.

We have a wide variety of ways we perform and keep backups for critical systems and data.

### Backups

- Online continuous backup - file level (double encryption)
- Virtual Hosts backup to Disk and Tape
  - [REDACTED] - two-week rotation

- [REDACTED] - 3-week rotation
- Monthly - [REDACTED] - 12-month rotation
- Shadow copy - every 2-3 hours during business hours
- Snapshots - SAN level - Depending on the server
  - hourly
  - daily
  - weekly
  - bi-weekly
  - monthly

During a recovery process event, we have a procedure at which we can determine the best path of actions to take place. Full recovery details are located in the Disaster Recovery Plan. The basic structured recovery process is as follows:

- Event
  1. Notifications
    - 1.1. IT personnel
    - 1.2. Affected users
  2. Determine scope
  3. Analyze best recovery actions
  4. Perform recovery
  5. Verify successful recovery
  6. Notify affected users
  7. Post-event analysis for any actions needed to prevent future occurrences

**Other Sections Specific to the Administrative Rule**

N/A

**Definitions**

N/A

**Interpretation of Administrative Rule**

The Chief Technology Officer maintains authority over this administrative rule.

**Cross Reference to Related Administrative Rules**

N/A

**Further Information**

Danial Dehaze, Executive Director of Infrastructure  
[ddehaze@cgcc.edu](mailto:ddehaze@cgcc.edu)  
(541) 506-6097

Aaron Churchwell, Information Systems Security Manager  
[achurchwell@cgcc.edu](mailto:achurchwell@cgcc.edu)  
(541) 506-6096

**Strategic Direction**

KFA 8: Information Technology Services  
Accreditation Standard Two

**Appendix**

N/A