



New River Community College

Information Technology Contingency and Disaster Recovery Plan

In compliance with ISO 27002:2013

Version: 2.5

Revised: 5/14/2025

Table of Contents

- Introduction 1
- Assumptions..... 1
- Information Technology Environment..... 2
- When an IT Disaster is Recognized 3
- IT Disaster Recovery Teams 3
 - IT Disaster Planning Coordinator 3
 - IT Emergency Management Team 4
 - IT Damage Assessment Team 5
 - IT Technical Support Team..... 5
 - Special Projects Team 6
 - Customer Support Team 7
- Emergency Response Procedures..... 7
 - Critical Systems and Applications 7
 - Recovery Procedures 8

Introduction

This Information Technology Disaster Recovery Plan was developed in conjunction with the IT Security Program in compliance with ISO 27002:2013 to allow a rapid and organized response to the full or partial destruction of the college's information technology capabilities. A disaster can be defined as a total or partial loss of any or all of the following: physical space, servers, workstations, network infrastructure equipment, personnel, software eradication, or hostile intrusion of the IT system resources resulting in an interruption of services. An IT Disaster Recovery Plan is a manual with procedures, responsibilities, and critical information required to execute a recovery of IT systems that support critical and essential business functions. The importance of planning for the eventuality of such losses is vital to limiting the amount of damage, decreasing the length of outages, and lowering the cost of recovery.

Assumptions

This plan was developed based on the following assumptions:

- One of the backup sites will survive the contingency.
- Backup media and documentation will be secure at the surviving site and will be made available as soon as possible.
- All resources and staff can be made available as soon as possible to implement the Contingency Management Plan.
- All members of the disaster recovery teams have the most current copies of the disaster recovery plan or they can access them online at <https://secure.navigateemergency.com/dms/dashboard> and on the college's Admin Plans secure web site.
- Users will continue to operate via a manual mode until IT services are restored.
- Service agreements with outside entities have been maintained.
- In the event of total or partial loss of the college's computer services personnel, assistance will be available from VCCS ITS Enterprises Services personnel to implement the Contingency Management Plan.
- In case of widespread regional disruptions access to emergency resources and personnel may be severely limited.

Information Technology Environment

New River Community College has implemented a first-class computer network composed of a Cisco switching and routing infrastructure that services desktop/laptop client computers and servers.

The internal cabling system uses unshielded category 5 cabling, and Cisco Distribution-Layer and Access-Layer switches. Inter-building cabling consists of multi-strand multi-mode optical fiber providing network switching and routing between all buildings on campus.

A Cisco router installed on campus in Dublin provides off-campus access via directly connected fiber optic cable to the Christiansburg site for NRCC network resources. These resources include email, Internet access, online instructional courses, files stored on the main-campus servers, and video conferencing access to the main campus for synchronous distance learning courses. A microwave link serves as a redundant connection between these two locations.

An additional Cisco router is installed to provide Voice over IP (VoIP) service between the NRCC main campus and the Virginia Community College System office in Richmond, Virginia and to other Virginia state colleges and agencies. This Cisco router provides access to the external public telephone system through a single PRI Digital line and support to an internal Cisco Call Manager IP Telephony system consisting of two (2) redundant servers. The NRCC IP telephone network consists of Cisco IP telephones, which provide phone access to faculty, staff, and classrooms. Two (2) redundant servers run Cisco Unity to provide voicemail services for all faculty and staff.

NRCC uses a Cisco edge router to connect directly to the VCCS MPLS network. Transport for Internet, Internet 2, and VCCS Enterprise Servers, including PeopleSoft SIS, is provided by a Lumos-branded fiber optic network, which has an access-speed rating of up to 300 Mbps.

The NRCC local area network currently consists of physical and virtual servers utilizing Windows and Linux platforms. There are over 1,200 PCs on the college network.

From their home or other off-campus locations, college administrators, faculty, and staff can use their personal Internet Service Provider (ISP) to connect to the NRCC web site, and the Blackboard distance-learning platform. Email for the college administrators, faculty, and staff is managed by Microsoft's cloud-based Office 365. Students have Web-based email maintained by Google and managed by the Virginia Community College System in Richmond, Virginia.

The College uses Tandberg video conferencing installed in four locations to deliver synchronous distance learning classes between the main campus and the off-campus sites.

When an IT Disaster is Recognized

In the event of an IT disaster or as notified following a business-wide disaster, the IT disaster planning coordinator, Tim Jones, Director for Information Technology and Facilities Services, will initiate IT disaster recovery procedures. If Mr. Jones is not available, the order of responsibility for initiating IT disaster recovery procedures is as follows: CISO, VP for Instruction and Student Services, College President. The IT disaster planning coordinator or substitute will secure a copy of the current disaster recovery plan. Current copies of the disaster recovery plan reside in the office of the Director for Information Technology and Facilities Services, the college's ISO, and online at <https://secure.navigateemergency.com/dms/dashboard> and on the college's Admin Plans secure web site. The IT disaster planning coordinator or substitute will perform a quick analysis of the situation and notify administrative staff at the VCCS and/or individual college staff as applicable, and computer customers and will call and place into service the appropriate IT disaster teams (description IT disaster teams listed below). The IT disaster planning coordinator or substitute will work with other disaster recovery teams to facilitate communication and coordination of efforts.

IT Disaster Recovery Teams

IT Disaster Recovery teams will provide coordination of critical resources between the time a disaster occurs and the restoration of service. Disaster recovery teams will be utilized to restore automated IT system services. The recovery teams will be led by the IT disaster planning coordinator and will participate in recovery activities based on the level of severity of the loss, recovery deemed necessary, and restoration order as identified in the Business Impact Analysis and Risk Assessment processes. The following teams have been identified to carry out the necessary recovery actions:

IT Disaster Planning Coordinator

The IT Disaster Planning Coordinators for the college are:

Primary: CIO - Director of Information Technology and Facilities Services

Secondary: CTO - Director of Technology Support Services

The responsibilities of the IT Disaster Planning Coordinator are:

1. Manage and coordinate all IT disaster plan activities.
2. Contact all IT disaster recovery team members involved in the recovery effort.
3. Ensure that all IT disaster recovery team members have a copy of the plan.
4. Appoint replacement staff if necessary.
5. Initiate tasks as delegated by IT disaster recovery team responsibilities.
6. Provide IT disaster recovery status via communication with college and/or VCCS administrators and other disaster recovery teams.
7. If necessary, assist planning for returning to normal conditions (renovations, new construction, etc.).

IT Emergency Management Team

The IT Management Team will consist of:

1. College President
2. VP for Finance and Administration
3. VP for Instruction and Student Services
4. Director for Information Technology and Facilities Services
5. Director for Technology Support Services
6. Director for Web Services
7. Facilities Services Director
8. Information Security Officer

The IT Management Team will be responsible for making decisions based on information received from the Damage Assessment Team and other emergency or security personnel. All members of the team should be familiar with the college's emergency and disaster recovery plan. The team will be responsible for the following:

1. Establishing a command and control center. The President's office is designated as the command and control center. In the event that the primary on-site command and control center is rendered unusable, the alternate on-site location is the Innovative Technology Center located in Martin Hall. If all on-site facilities are rendered unusable, the command and control center will be established at the New River Valley Mall site in Christiansburg, Virginia.
2. Contacting and briefing the following management on the status of the disaster:
 - a. Dean of Arts and Sciences
 - b. Dean of Business and Technologies
 - c. Dean of Health Sciences
 - d. Director of Distance Education
 - e. Director of Admissions, Records, and Student Services
 - f. Vice President for Workforce Development
3. Notifying the following individuals and vendors where appropriate to restore services to the damaged areas (Refer to Emergency Notification Telephone List):
 - a. VCCS Chancellor
 - b. VCCS Assistant Vice Chancellor for Information Technology Services
 - c. VCCS ITS Enterprise Services
 - d. Miscellaneous vendors as needed
4. Determine the priorities. Make decisions on recovery steps using the IT Disaster Recovery Plan and any other information that may be available to the Management Team.
5. Appoint replacement staff if required
6. Establish a timetable for restoring normal operations.
7. Implement emergency procurement procedures consistent with the Department of General Services' Agency Procurement and Surplus Property Manual.

IT Damage Assessment Team

The IT Damage Assessment Team will consist of:

1. Director for Information Technology and Facilities Services
2. Director of Technology Support Services
3. Director of Network Services
4. Director of Web Services
5. Facilities Services Director
6. Coordinator of Emergency Response and Campus Security
7. Current Vendors

The Damage Assessment Team is responsible for the following:

1. Ascertain when entry to the facility can safely be made to retrieve backup media.
2. Contact all vendors to meet at the damaged facility to access the damage on information technology resources.
 - a. Identification of damaged resources
 - b. Identification of resources that may be salvageable
 - c. Identification of critical applications that require processing capabilities as identified in the Business Impact Analysis and Risk Assessment processes
 - d. Feasibility of restoring service on an interim basis to provide processing of critical applications at current location
 - e. Status of vendor support requests
 - f. Requirements for site security

IT Technical Support Team

1. Director for Information Technology and Facilities Services
2. Director of Technical Support Services
3. Director of Web Services
4. VCCS Information Security Officer
5. VCCS Customer Services

The responsibilities of the IT Technical Support Team will be as follows:

1. Using information from the Damage Assessment Team and Management Team, make specific assignment of responsibilities as needed to members of the Technical Support Team. Specific areas of assignment may include the following:
 - a. Work with the IT Emergency Management Team to conduct an on-site assessment of the damaged area to determine the condition of IT resources.
 - b. Determine what computer hardware/software have been damaged.
 - c. Review the risk assessment analysis and business impact analysis and determine what the critical/non-critical applications are and to determine who is responsible for each application.
 - d. List procedures to create a new environment for the hardware or for the purchase of new hardware.
 - e. List procedures to restore critical software/applications as identified in the Business Impact Analysis and Risk Assessment processes.
 - f. List procedures to restore non-critical software/applications.

- g. Contact application owners to determine their role in the recovery process. Refer to the Business Impact Analysis list.
 - h. Staffing off-site recovery facilities.
 - i. Restoration of backup tapes to disk at the backup site.
 - j. Restoration of wide area telecommunication (WAN) links.
 - k. Restoration of local area network (LAN) communications.
 - l. Restoration of the campus Cisco Call Manager IP phone system.
 - m. Salvage usable equipment, software, and documentation.
 - n. Procurement of replacement equipment, software, and services.
 - o. Transportation of equipment, media, and documents.
 - p. Reestablish terminal address dependent access privileges within VCCS and VITA.
2. Schedule, coordinate, and communicate with other contingency teams, users, vendors, and VCCS ITS Enterprise Services personnel as required. Refer to Emergency Notification Telephone List.
 3. Review pre-contingency information technology environment.
 - a. Installed Equipment List
 - b. Installed Software List

Special Projects Team

The Special Projects Team will consist of:

1. IT Staff
2. Web Master
3. Procurement Staff
4. Accounting Staff
5. Fixed Asset Coordinator
6. Facilities Staff
7. Security Staff
8. Administrative Support Staff

Responsibilities of the Special Projects Team may include:

1. Providing transportation to and from backup facilities, external vendors or other off-site locations.
2. Assisting in making telephone calls as needed.
3. Coordinating packing and moving supplies as needed.
4. Acquiring emergency purchasing means (i.e. assigning purchasing charge card or delegated purchasing authority) or being available to purchase goods or services as needed.
5. Providing administrative support as needed.

Customer Support Team

The Customer Support Team will consist of:

1. IT Disaster Planning Coordinator
2. Director of Technology Support Services
3. Director of Network Services
4. Director of Web Services
5. Instructional Media Services Technician
6. Administrative Support Staff

Responsibilities of the Customer Support Team may include:

1. Notifying IT customers of the disaster and giving them a timeframe for recovery.
2. Assisting customers in developing manual procedures to accomplish work if resources are unavailable for a long period of time.
3. Assisting users with hardware and software restoration or relocation to an alternate office site.

Emergency Response Procedures

In the event of an emergency, the procedures for returning to normal operations are explained below. The critical applications listed below are to be addressed and operations restored as described in the Business Impact Analysis.

Critical Systems and Applications

The College's major applications and systems were assessed in the Business Impact Analysis developed in conjunction with this plan. During that assessment process, the following systems and applications were identified as being critical to the college's continued operation:

System/Application Name

1. Infrastructure
 - a. Backup EXEC (data backups)
 - b. Cisco Network (routers, switches, etc.)
 - c. Electronic Classrooms (Crestron Programming and Fusion Server)
 - d. IP Telephony (telephone system components)
 - e. Media Services production equipment
 - f. Network Servers (web, database, file servers)
 - g. Network connection to Mall site
 - h. WAN (VCCS Wide Area Network)/Internet
 - i. Local AD (Active Directory authentication/permissions)
 - j. EAD (Enterprise Active Directory authentication/permissions)
2. Desktop computer support and PC applications
 - a. DELL/KACE (patch management)
 - b. Microsoft Office (Excel, Outlook, PowerPoint, Word, etc.)
 - c. Office 365 (Faculty/Staff Email)
 - d. Student Lab Applications (all lab workstations fully functional)
 - e. Faculty/Staff Desktop Applications and Data (all faculty/staff workstations fully functional)
 - f. RAdmin – Remote access
3. State Applications
 - a. CIPPS – Commonwealth Integrated Personnel and Payroll System - HR

- b. eVA - Purchasing
- c. Cardinal – (replacement for CARS) Accounting, Reporting - Business Office
- d. Everbridged ENS – Emergency Notification System
- e. PMIS – Personnel Management Information System – HR
- 4. VCCS Enterprise Applications
 - a. Admissions Application
 - b. Blackboard Learn
 - c. Image Now - Document Management
 - d. Gmail - Student Email
 - e. Library Services
 - i. ALEPH – Library Automated System
 - ii. MetaLib – Search System
 - iii. SFX – OpenURL resolver
 - f. myVCCS (Enterprise Application Portal)
 - g. PeopleSoft AIS – AP, AR, Billing, Cashier, Refunds
 - h. PeopleSoft HR – Benefits, Payroll, T&L
 - i. PeopleSoft SIS – A&R, Financial Aid, Student Financials, Veterans
 - j. Query Databases – SISQUERY, HRQUERY
 - k. Virginia Wizard – Students (career/interest assessment)
 - l. WES – Workforce Enterprise System
- 5. Local Web Applications
 - a. CLAS – Connecting Learning Assets to Students
 - b. DE Intranet – DE office support
 - c. FA - Summer FA and Federal Direct Student Loan applications, CWSP management.
 - d. IIWS – Instructor Initiated Withdrawal System
 - e. NETSPACE – Strategic Planning/Project Induction/Funding Requests
 - f. OTIS – Open Text Initiative System
 - g. PAS – Productivity Analysis System + Workload/Payroll
 - h. RADSS – Research Assessment Data Support System
 - i. UL - Unified Login (NRCC’s local application portal)
 - j. Web Schedule (public facing web schedule and administration)
- 6. NRCC Website
 - a. Public Facing Information pages
 - b. Platform for local Web-based applications (see above)

Identification and ranking of the most critical applications will need to be performed when a disaster occurs. The criticality of the application will depend upon the point in an application's processing cycle and the degree of damage sustained as the result of the disaster.

Recovery Procedures