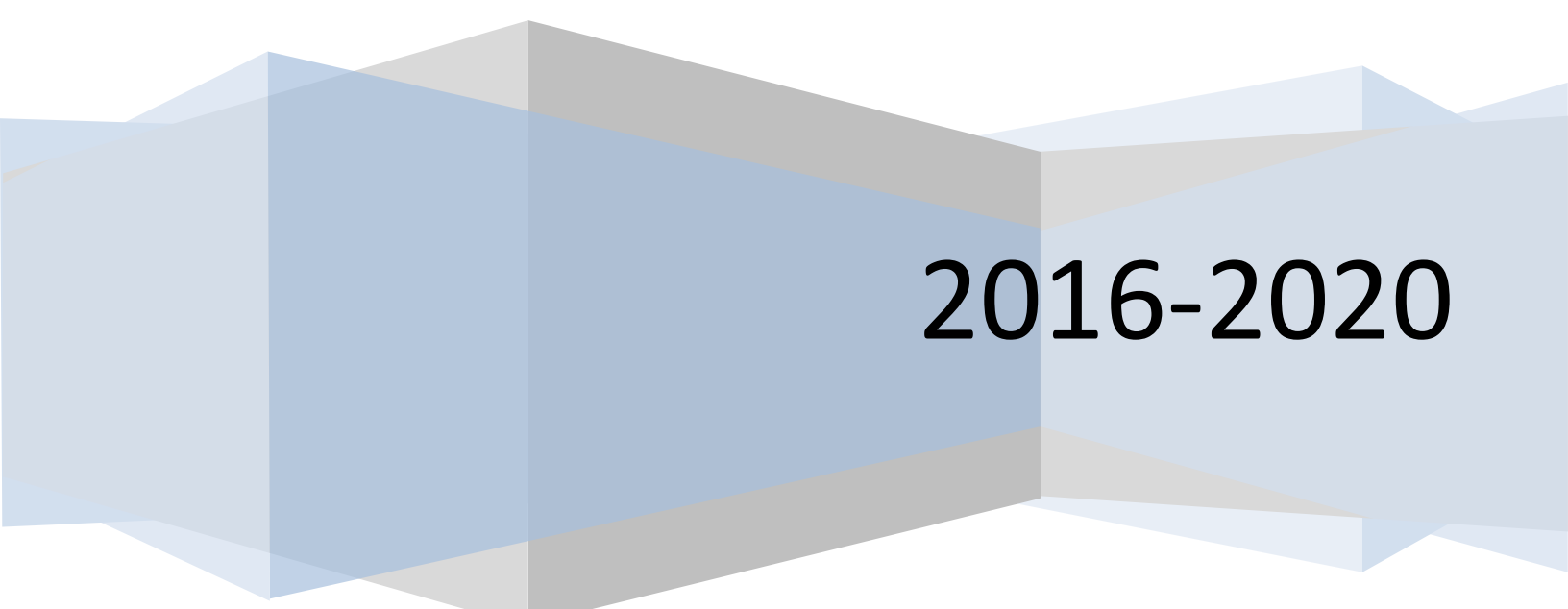


Grayson College

Technology Plan

2016-2020

Including Grayson College Disaster Recovery Plan



2016-2020

Technology Plan 2016 - 2020

Information and instructional technologies are now essential components to fulfilling the mission of a college. Technology is changing how we access, organize, analyze, and process information. It is considered instrumental for improving information exchange, enhancing teaching and learning, empowering research, and increasing productivity. Technology is changing how we conduct business and how we communicate. Technology's influence, impact, and presence are reshaping our society, our commerce, our work life, our leisure life, and our education.

The growth and expansion of technology brings continuous change. Planning for technology is challenging when the landscape changes every day. However, an organization needs to chart strategic principles and objectives to shape tactical plans and approaches as it explores, evaluates, selects, implements, and leverages technology. *Technology Plan 2016 - 2020* presents the college's technology strategic principles and objectives and suggests the next steps and initiatives for technology at Grayson College.

Strategic Planning Process

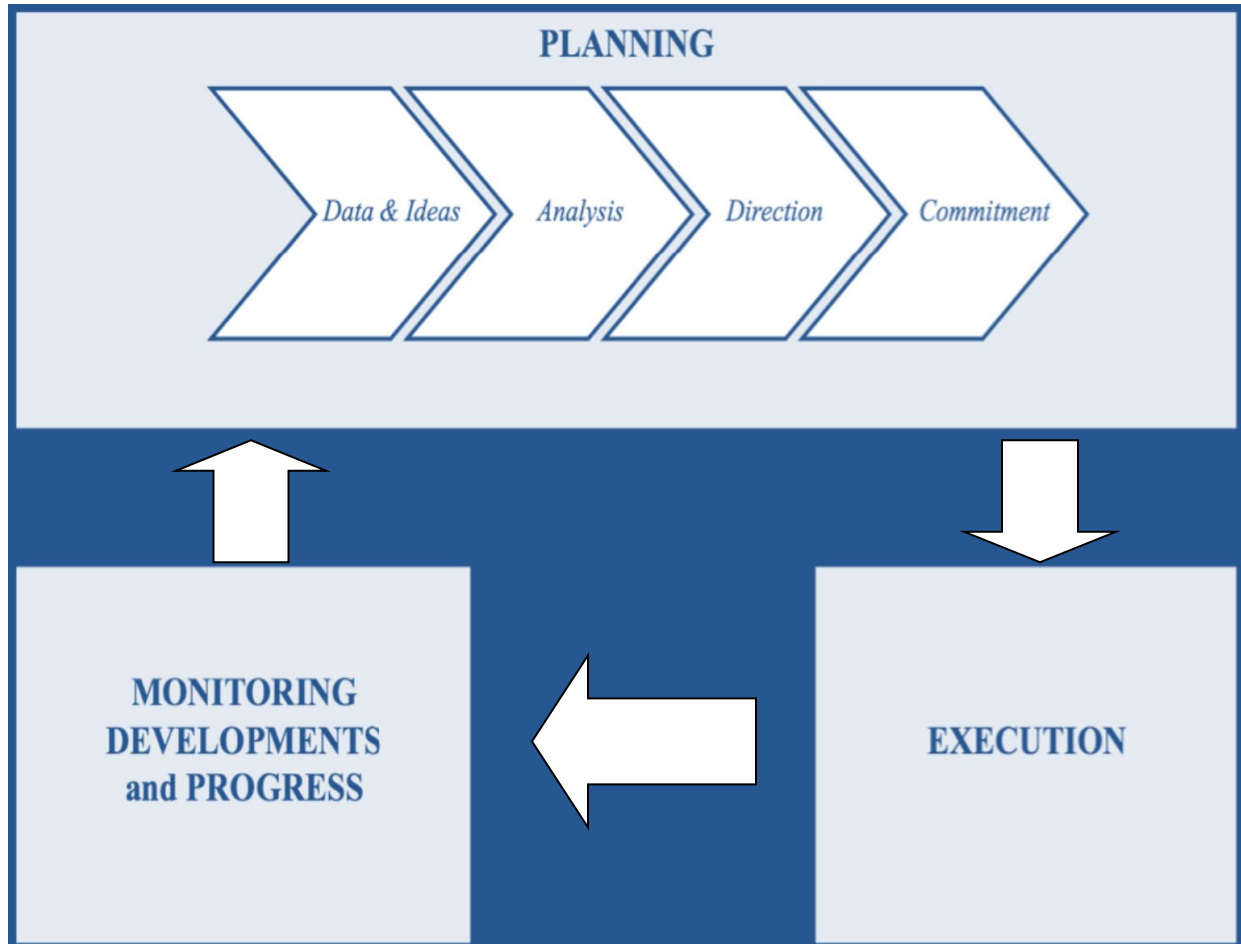
Technology should be readily accessible to all students, faculty, and staff of the college. The college will insure that all students, faculty, and staff have required access to computers, software, and technology services. Capabilities should be developed to provide fully functional accessibility to the entire college community both on and off the college's campus.

Planning

The technology objectives of the college need to be aligned with institutional priorities and the technology planning process of the college needs to insure a high level of inclusion and interaction. The technology planning process provides an opportunity to:

- ▶ Determine the fundamental technology directions of the college.
- ▶ Identify key strategies in taking the next steps.
- ▶ Clarify the tactical plans and actions needed to help departments, divisions, and the college, achieve their broad missions and goals.
- ▶ Disseminate knowledge about technology milestones, existing technology services, technology needs, and technology constraints.
- ▶ Evaluate current initiatives, services, and practices; revise and expand services as needed. Articulate what leadership and services the campus can expect from college technology organizations.

Information Technology Strategic Planning Process



Impact of Technology Advances

Computational devices will continue to physically and logically converge. Voice, data, video, music, chat, IM, web, GPS, TV, radio, gaming systems, desktop, laptop, notebook, pocket, ultra mobiles, wearable, embedded, teleconferencing, etc. will continue to come together. Classrooms of the future will be radically different because of this device convergence—making the classroom without walls more of a reality than it already is.

Networks will physically and logically converge, enabling seamless application transfer with no loss of functionality. Networks are now distinct with different vendors providing voice, video, and data services resulting in problems and gaps in services. In the future those services will function seamlessly through network convergence.

Social interactivity will dominate, changing classroom models further as students from elementary school through high school through college, and then in the workplace, grow up on instant messaging, chat, iTunes, Facebook, YouTube, Twitter, interactive video gaming, etc.

Digital networks have evolved from carrying data in a purely transactional sense to facilitating social interaction. The Internet is also increasingly seen as a resource for social interaction rather than just information transport for a generation that is already cyber-savvy.

Technology Direction

The college's technology direction is organized around certain core activities: teaching, learning, student life, research, and administrative support. The use of technology for each of these areas depends on a solid technology infrastructure with appropriate support services. It is expected that faculty and staff will demand more sophisticated technology opportunities to handle their responsibilities. Additionally, an increasing number of faculty, students, and staff will come to Grayson College with high expectations of information technology. These factors place greater demand on the college's capabilities and resources.

The community that we serve is large and diverse with information technology needs ranging from simple network access to sophisticated enterprise resource management systems. The university systems that we architect and provide must address the diverse requirements of the university constituencies. These systems must be provided in a way that is easily accessible for our community and can be delivered reliably.

The Community We Serve

- ▶ Students
- ▶ Faculty
- ▶ Staff
- ▶ Administrators (executive leadership)
- ▶ Alumni
- ▶ Guests & Visitors (prospective students, vendors, visiting professors, parents)
- ▶ Grayson County community
- ▶ State of Texas Organizations
- ▶ Regional, National, and Global Organizations

Key Strategies

Adopting planning strategies assists GC in achieving the overall technology goal of increasing access to electronic data for retrieval of up-to-date information to increase efficiency, productivity, and communication. Planning strategies also provide students with access to state-of-the-art technology, helping create a premier learning-centered environment at Grayson College.

The MyViking Portal, GC Faculty Portal, Canvas and the GC website facilitate anytime, anyplace access for students to register, schedule classes, view grades, view transcripts, pay bills, utilize campus calendars, and send email. Enabling technology access for faculty and staff allows them to better support students and prospective students.

Student learning drives project priorities. Every effort is made to meet student needs. These needs include anytime, anywhere access, seamless services, smart classrooms, and premier online technology allowing faculty to engage students in interactive learning.

Administrative support leads to technology innovation. Technology is a valuable tool enhanced by the competency of the Information Technology department who must maintain regular technology replacement cycles and provide consistent technical support in order to preserve the quality of GC's technology.

Teamwork builds on collaborative decision-making. Planning, decisions, and implementation are accomplished with input from various campus groups. Project-based teams help in the decision making process and participate in the implementation of decisions. A team approach is key to the implementation and continued support of MyViking Portal, CAMS, and Canvas course management system.

Innovation relies on informed research. The Information Technology Department gathers information on new technologies and processes from listservs, conferences, webcasts, scholarly research journals, vendor demonstrations, online demos, and peer networking in order to maintain the high quality of GC's Information Technology services.

Adaptations evolve as technology changes. As plans are designed and implementation is carried forward, ongoing changes are made to produce a stronger project. As a result of innovation and investigation the final products produced are improved.

Standards determine purchasing. Hardware and software purchases that adhere to common standards produce better support and training for users. Efficient deployment is also ensured when those purchases adhere to common standards. Standardized operating systems allow maximizing time and talents of support service staff.

Projects are phased in according to specified timelines. This acquisition and implementation approach allows for manageable project timelines and regulated monetary expenditures.

Communication promotes successful implementation. Technology plans and implementation are communicated through multiple venues. Faculty forums, committee representation, presentations, campus-wide email, and the web are vehicles for communicating with the Grayson College community.

Tactical Plans and Actions

Student Learning

Because teaching and learning profit through the use of technology, Grayson College is committed to enabling faculty to appropriately integrate technology into the curriculum through special incentives and technology equipment upgrades that facilitate creating a premier, learning-centered environment at GC.

Administrative Support

The Information Technology Department will continue to provide an infrastructure for interaction, investigation, and collaboration for faculty, staff, and students. IT promises to be a transformative agent that not only enhances traditional modes of teaching and learning, but also enables new methods of teaching and learning through technology. The Grayson College network infrastructure will continue to support teaching, learning, and administrative support services.

Collaborative Decision Making through Teamwork

Planning for future technology projects will continue to be based on a collaborative and team building model in order to foster informed decision making through the combined efforts of the Grayson College community.

Innovation through Research

Technology advances create challenges for the GC Information Technology team as the role of IT has moved from enabling day-to-day transactions to collaborating on strategic decision making. In order to avoid being locked into outdated and inefficient technology IT will allocate time, resources, and access to ensure ongoing professional growth in technology fluency and integration. This can be accomplished through participation in learning communities that stimulate, nurture, and support administrators, faculty, and staff in the study and use of technology. In addition, IT will stay abreast of educational research and emerging trends regarding effective use of technology and encourage evaluation of new technologies for their potential to improve student learning.

Adapt to Emerging Technology

Providing an IT infrastructure that can evolve and adapt to emerging technologies is imperative as GC strives to create a college without walls and one that focuses on student-centered learning in a fast-changing technology climate. The rapid growth of technologies such as wireless communications, mobile commerce, inter-organizational systems, and Web 2.0 offer educational and business opportunities that operate outside of the traditional technology boundaries. As these and other emerging technologies become widely used, Grayson College will continue updating and replacing existing technologies in order to adapt.

Maintain Campus-Wide Technology Standards

Establishing and maintaining a robust infrastructure for technology including integrated technology systems to support management, operations, teaching, and learning depends upon technology systems consisting of common standards to ensure reliability and security. IT leadership will promote comprehensive integration of technology to achieve excellence while educating stakeholders on the importance of maximizing the use of technology resources to meet and exceed learning goals and to support effective instructional practice.

Project Timelines

Successful technology project implementation depends upon thorough and continuous planning and goal reassessment. Estimating project timelines includes a schedule of task execution from which the endpoint and the cost can be calculated. Information Technology project timelines will include project schedules with allowances for schedule risk, internal complications, and other risks to the project schedules. Also included in project timelines will be technical and user requirements. Considering these criteria when estimating timelines will ensure maximum success for technology project implementation.

Implementation with Communication

Utilizing communication in planning, decision making, and project implementation builds a strong team effort that results in collaboration to ensure successful technology project implementation. IT will continue to solicit input from various campus groups to augment Information Technology's expertise in order to find technology solutions that result in efficient operations and maximize the use of college resources and personnel.

Technology Services and Milestones

The Key Services We Provide

- ▶ Wide Area Network comprising multiple campuses utilizing Voice over IP and Local Area Networks
- ▶ Business system processing of transactions
- ▶ Trusted technology, policy, and security expertise
- ▶ Access to data
- ▶ Tools that assimilate data into information
- ▶ Consulting on information, communication and instructional technology, and future directions
- ▶ Engines and tools for collaboration for the information technology community
- ▶ Physical and logical communications
- ▶ Computing cycles
- ▶ Physical storage; back-up; redundancy
- ▶ Academic computing assistance
- ▶ Secure, copyright-managed streaming and new media services and support
- ▶ Design, implementation, and technical and end-user support of physical and online learning environments
- ▶ Desktop and information technology support

Web Redesign

A major redesign of the College's website was undertaken which updated the look and navigation of the site with new functionality, content enhancements, and innovative features. The new design included consistent left-side navigation for all pages in order to deliver user friendly access to college-wide services and information throughout the site. A top navigation menu provides easy access to information and highlights College functions, departments, and featured services. The implementation of Google Search adds to the overall search functionality

of the Web site. The Web site contains a fresh color palette in addition to text only, printer friendly, and text resizing features to enhance accessibility and advance the Information Technology departments strategy of creating education without walls.

Email Retention Policy

Grayson College implemented an email retention policy containing specific parameters for email deletion and retention, the *Grayson College Information Handling Backup and Retention Standard* provides detailed guidance.

If an email message:

was created or received in the transaction of business,

was retained as evidence of official policies/decisions, or

has historical significance valuable informational content

it is considered a College record and is subject to the same retention period as the paper equivalent (i.e. email may be equivalent to formal correspondence). As such it may need to be retained for longer than an email system is capable of retaining it. It is the responsibility of the sender/recipient to determine if a particular email message constitutes a College record.

Email messages which require long-term retention should be either retained electronically on retrievable media or printed, including all header and transmission information, and filed with their electronic or paper equivalents by the sender/recipient.

In a court of law, liability can become involved when such documents (paper or electronic) are not available to be provided. Be aware that your decision to retain or destroy an email message may become an issue in a court situation.

Estudias

Estudias coordinates and assesses enrollment management efforts before, during, and after a semester. Integrates data from multiple data sources: National Student Clearinghouse, CCSSE/NSSE, Excel, etc. Pre-bundled with reports and metrics currently in use at other institutions.

My Viking Portal (CAMS)

The MyViking Portal provides web-based, self-service, e-learning, online communications, and community-building tools through a single site, with a single log-on. MyViking provides personalized, one-stop access to academic and administrative data anytime, anywhere.

Active Directory (Single Sign-On)

Grayson College maintains an Active Directory domain infrastructure to manage and control access to all of our servers, and desktop systems, used by faculty and staff. We maintain group policies and user access control for all users in the domain. Since all enterprise resources are part of the domain, once a user has been granted access, they can access that resource, even on another server, without having to login again. We also use AD to integrate with Google to manage our email accounts and passwords.

Strategic Planning Online (SPOL)

SPOL automates the strategic planning, budgeting, and assessment cycle. Allows GC personnel to manage strategic objectives, institutional outcomes, and accreditation requirements while ensuring that budgets are supporting the QEP effort.

Point-of-Sale for Food Service

The POS enables administration of dining services with unlimited options for accounts, plans, menus and point-of-sale selections. In addition, reporting and management controls improve accountability.

Follett Point-of-Sale for Bookstore

The Follett POS integrates entire store operations, including retail accounting, EDI and point of sale into one system. Maximizes data analysis capabilities and performance.

Microsoft Office 365

Faculty and staff computers are equipped with Office 2016. In addition, all faculty, staff, and students have access to Office 365 for free on up to 5 devices. Regularly scheduled training opportunities are available to faculty and staff with future training sessions to be developed based on faculty and staff needs.

Technology Initiatives, Services, and Practices

Reliable Technology Services

Information and instructional technology accessibility will be delivered via a secure, solidly established, centrally operated, redundant, and robust network and computer infrastructure. The college will continually explore opportunities for students, faculty, staff, prospective students, and the public to access to information and technology services. In addition, the college will provide a regular assessment of its technology infrastructure and support to insure that the resources and services meet the needs of the campus community. Guidance on this process can be found in the *Grayson College Written Information Security Program*.

Replacement Strategy

The college will continue to upgrade, maintain, and replace computer hardware, computer workstations, classroom technology, audio/visual equipment, network infrastructure, telecommunication infrastructure, computer servers, and software on a regular planned timetable so that the college's technology services will be reliable and will provide state of the art capabilities and features.

Technology Standards

Grayson College will continue to build and maintain a campus infrastructure with adequate bandwidth, reliability, redundancy, services, and security to support college technology needs. The college will maintain campus-wide standards for computing hardware, classroom audio/visual technology, software, and services to facilitate collaboration, to maintain state of the art computer technology, to simplify upgrades, and to simplify support and training.

Provide Technology Enhanced Education

Grayson College is committed to a learning-centered environment. Studies continue to show that both teaching and learning can benefit through the use of technology. Through the use of Canvas and the Internet, faculty and students have ever-expanding access to each other via e-mail, chat, and discussions. As technology becomes more embedded in instruction, more training and resources will be required from the college as faculty integrate the use of technology in teaching and learning. In order to continue supporting GC faculty as they provide technology enhanced education, IT will equip campus classrooms and laboratories for specific delivery needs and at a necessary level for instructional effectiveness and efficiency. These rooms will also be continually upgraded on an as-needed basis in order to continue to support the goal of technology enhanced education.

Improve College Business Operations

Technology is transforming the creation of new products and services, the organization and presentation of business information, and the accessibility and delivery of services. The power and capabilities of technology in business operations has also changed expectations. Grayson College is ready to meet new and heightened expectations for customer service utilizing technology to transform the productivity and efficiency of the college, to enable the collaboration of organizational units, to improve the design and flow of operations, to enhance the interaction with business partners and suppliers, and to continue providing exceptional customer service to students and the community.

GC's Commitment to Information Access and Services

Grayson College will continue to implement and improve information and technology systems that provide enhanced information access and services to faculty, staff, and students. Through the use of technology systems such as the MyViking Portal, Canvas, SPOL, Estudias, and the point-of-sale systems, the academic, admissions, registration, and payment processes that students experience are conducted more efficiently. In addition, utilizing these technology systems provides Grayson College with the ability to evaluate, assess, and improve those processes regularly.

The information and technology systems also provide information and services for faculty and advisors to improve how they perform various functions such as teaching, advising, receiving class roster information, submitting grades, and viewing course and instructor schedules. These systems are flexible, which permits the college to review and easily redesign business processes in order to improve productivity and customer service capabilities. They also provide a convenient means for students to conduct business with GC. Continual improvement of GC's information and technology systems ensures that the college will continue to provide exceptional technology and information services for our students, our faculty, and our staff in order to become a premier, learner-centered institution.

GC

IT Disaster Recovery Plan

Document Change Page

Revision	Prepared Date	Approved Date	Reason for Change
Original	09-25-2009		Draft IT Recovery Plan for review
1.0	09-25-2017		Update IT Recovery Plan Dates
1.1	09-09-19		Appendix C renamed to Appendix B
1.2	09-11-19		Updated Phone Services & 911 Info
1.3	12-11-20		Updated References to guiding procedures throughout document.

**Grayson College
Information Technology (IT)
Disaster Recovery Plan
Table of Contents**

1.0 Introduction 15

2.0 Objectives..... 15

3.0 Scope..... 15

4.0 Assumptions..... 16

5.0 Definitions..... 16

6.0 General Disaster Response and Recovery Guidelines 17

7.0 IT Risk Assessment

 7.1 Level 1 Computer Services Area and Central Computer Room 17

 7.2 Level 2 GC Telecommunications 20

 7.3 Level 2 911 Emergency Services 22

 7.4 Level 2 Network Services 23

 7.5 Level 2 Cable Plant 26

 7.6 Level 3 File and Print Services..... 27

 7.7 Level 3 Enterprise Resource Planning Services (CAMS)..... 29

 7.8 Level 3 Email Services 30

 7.9 Level 3 Web Services..... 32

 7.10 Level 3 Campus Card Services..... 33

7.11 Level 3 Residential Network Computer Services (ResNet) 34

7.12 Level 3 Academic Instructional Technology Classrooms 35

7.13 Level 3 Student Computer Laboratory Services..... 36

8.0 Maintenance of the IT Disaster Recovery Plan 30

9.0 Appendices

Appendix A: Disaster Recovery Action Items

Appendix B: Vendor Contact Information

1.0 INTRODUCTION

Grayson College (GC) is a two year, Texas, public college that offers undergraduate Liberal Arts and Sciences, Teacher Preparation, and Business degree programs; and also offers two year transfer programs as directed by our community college role and mission. Over time, Information Technology (IT) services have become critical to performing the educational mission of the college. As a result of this ever-increasing reliance on technology, IT services require a comprehensive Disaster Recovery Plan to assure these services can be re-established quickly and completely in event of a disaster.

The GC Disaster Recovery Plan summarizes the results of a comprehensive risk analysis conducted for all IT services; it provides general steps that will be taken in event of a disaster to restore IT functions; and it provides recommendations for “hardening” of the IT infrastructure that require executive-level management approval and additional funding to implement.

1.0 OBJECTIVES

The primary objective of this Disaster Recovery Plan is to help ensure college business continuity by providing the ability to successfully recover computer services in the event of a disaster.

Specific goals of this plan relative to an emergency include:

- Detailing a general course of action to follow in the event of a disaster
- Minimizing confusion, errors, and expense to the college
- Implementing a quick and complete recovery of services

Secondary objectives of this Plan are:

- Reducing risks of loss of services
- Providing ongoing protection of institutional assets
- Ensuring the continued viability of this plan

3.0 SCOPE

This plan will only address the recovery of systems under the direct control of the Computer Services Department that are considered critical for business continuity. Also, given the uncertain impact of a given incident or disaster, it is not the intent of this document to provide specific recovery instructions for every system. Rather, this document will outline a general recovery process which will lead to development of specific responses to any given incident or disaster.

Three levels of risk, based on severity to campus operations, have been identified. A Level 1 risk is associated with the Computer Services area and central computer room which house the campus servers, router, VOIP, and serves as the primary hub for campus electronic and voice communications and connectivity.

A Level 2 risk is associated with the campus network infrastructure and the telephone public exchange (VOIP). The final risk level, Level 3, is associated with risks specific to unique applications or functionality. Though risk at all levels must be addressed for disaster recovery purposes, Level 1 risks will be given increased priority over other levels. The same holds true for Level 2 versus Level 3 risks.

The following major service areas are addressed in this plan:

Level 1

- Computer Services Area & Central Computer Room

Level 2

- Central Telephone Services
- 911 Emergency Services
- Network Infrastructure and Services
- Cable Plant

Level 3

- File & Print Services
- ERP Services (CAMS)
- Email Services
- Web Services
- Campus Card Services
- Student Residential Network Computer Services
- Technology Enhanced Classroom Support
- Student Computer Lab Services

4.0 ASSUMPTIONS

This disaster recovery plan is based on the following assumptions:

- The safety of students, staff, and faculty is of paramount; the safeguard of such will supersede concerns specific to hardware, software, and other recovery needs.
- Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in this IT Disaster Recovery Plan will be made available.
- Depending on the severity of the disaster, other departments/divisions on campus maybe required to modify their operations to accommodate changes in system performance, computer availability and physical location until a full recovery has been completed. The GC Executive Council will encourage campus departments to have contingency or business continuity plans for their operations, which include operating without IT systems for an extended period of time.

5.0 DEFINITIONS

The following definitions pertain to their use in this IT Disaster Recovery Plan:

Backup/Recovery Tapes: Copies of all software and data located on the central servers, which are used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.

Disaster: A significant or unusual incident that has long-term implications to business continuity and the ongoing operations of GC.

Incident: An event which impacts a specific IT service or server.

Level 1 Risk: Risk associated with the most critical IT services/capabilities, based upon impact to the campus if the service or capability were lost.

Level 2 Risk: Risk associated with critical IT services/capabilities, based upon impact to the campus if the service or capability were lost.

Level 3 Risk: Risk associated with the loss of selected applications/functionality.

6.0 GENERAL DISASTER RESPONSE & RECOVERY GUIDELINES

1. In the event of a disaster, the VP of Information Technology will notify the three primary IT Disaster Recovery Teams; network, administrative and telecommunications (see Appendix A, IT Disaster Recovery Teams).
2. Appropriate steps will be taken to safeguard personnel and minimize damage to any related equipment and/or software.
3. A damage assessment will be conducted by each team and recommendations made to the VP of Information Technology for recovery of impacted services.
4. Individuals required to assist in recovery of these services will be identified.
5. The campus will be informed as to IT system degradation and restrictions on IT usage and/or availability.
6. The VP of Information Technology will develop an overall IT recovery plan and schedule, focusing on highest priorities of the campus infrastructure, first, as defined by the Executive Council.
7. Necessary software and hardware replacement will be coordinated with vendors and the GC Purchasing Office, as required.
8. The VP of Information Technology will oversee the recovery of campus IT services based on established priorities.
9. The VP of Information Technology will ensure that IT recovery efforts are properly coordinated with other campus recovery efforts.
10. The VP of Information Technology will communicate recovery status updates to the GC Executive Council and campus at large.
11. The VP of Information Technology will verify restoration of the IT infrastructure to pre-disaster functionality.

7.0 IT RISK ASSESSMENT

7.1 Level 1 - Computer Services (CS) Area and Central Computer Room

7.1.1 General

Computer Services is housed in a one story, concrete, structure located on the north end of campus, and the Computer Services staff is also housed in that facility. The Central Computer Room houses the main campus servers and router; the phone switch (VOIP) and peripheral servers, such as the web servers, CAMS, and all servers providing resources for educational and administrative tasks at GC. It is the location where all data and transmitted communications for Grayson College are redirected, combined, stored and retrieved. There is no off-site backup facility, currently identified, that could entirely replace the functions of the Central Computer Room if it is rendered inoperable by an environmental or manmade disaster. The Van Alstyne facility however could be used to restore our on-line presence by hosting our virtual machines, allowing students, faculty, and staff to continue with on-line activities.

7.1.1 Risk Assessment

7.1.1.1 Physical/Security Risks

The Computer Services area can be accessed through three doors. Each door is keyed to a unique Computer Services key; a campus master key will not open the Computer Services doors. There are a large number of windows on the both sides of the building which are susceptible to breakage and possible unauthorized entry. Many of the windows have screws or bolts on the outside frames, allowing for potentially undetected intrusion into the building. There is no alarm system for the building doors or windows. Periodically officers from the campus Public Safety Office will ensure that the building doors are secured. Entrance to the Central Computer room is through two locked doors; keyed with Computer Services, unique keys; the room is comprised of concrete walls with windows on the east facing side. The Central Computer Room is not directly accessible through the three entry doors into Computer Services. There is no video surveillance inside the computer room.

7.1.1.2 Environmental Risks

Rain

- The CS building has a flat roof; the roof has leaked into the Central Computer Room in the past.
- There are no environmental sensing devices installed in the Computer Room to detect water leakage. If a leak were to occur over a weekend, CS personnel may not be aware of it until the following Monday, possibly too late to mitigate equipment damage.

Flooding

- Offices would be impacted in the event of flooding. VOIP batteries and UPSs are located in the Central Computer Room and would be ruined if flooding were to occur.
- The building generator is located at ground level and is susceptible to a flooding risk.

Fire

- Though the building structure is concrete, it houses a large number of desktop computers, a paper storage area, a VOIP battery room, and individual cubicles which contain documents, books and equipment.

- The Computer Room contains large quantities of equipment, but minimal combustibles such as papers or documents – widespread fire is not likely; however, small, contained fires are possible in the wiring and equipment.
- Storage of combustibles (cardboard, paper, plastics, liquids) is not allowed in the Computer Room.
- There is no fire suppression system in the Computer Room to reduce damage to equipment.

Extreme Temperatures

- Primary and backup air conditioners are available to cool the Central Computer Room. Either system is capable of providing the necessary cooling for the room. Both the primary and the backup air conditioners are powered by the primary electrical system with no backups.
- Computer Room air conditioner units have heaters and the computers produce heat, so risk of too low a temperature is minimal.

Natural Disasters (earthquake, tornado, high winds)

The CS building is a solidly constructed concrete structure which protects personnel and equipment from high winds.

7.1.1.3 Internal Systems Risk

- Power is provided to the CS building from TXU Energy through the regular power grid. The building has 3-phase power utilizing transformers to provide power for the air conditioners and multiple step-down transformers to provide power for equipment in the computer room.
- The main building transformer and entry wiring is located on the west exterior wall of the Computer Services building.
- Essential computers and equipment have battery UPSs to maintain power until the generator can run up in the event of a power outage. Many of the UPSs are operating well-beyond their recommended useful life and need to be replaced.

7.1.1.4 External Systems Risk

- Operation of the Central Computing Room is highly dependent upon the external campus cable plant which provides fiber and copper lines to carry data and telecommunication services.
- The cable plant was upgraded in CY2000 as part of the campus cable plant capital project. The cable plant is estimated to have a ten year life expectancy.
- Copper wiring and fiber optic cable is run in underground conduit that can be accessed via manholes.

7.1.2 Recovery Planning

- Recovery decisions will be based on the extent of the damage to the CS area and central computing room. A backup computing facility does not currently exist, so if the central computing room remains habitable, every effort will be made to re-establish services in the same area.

- If the central computer room is not habitable, the IDF room in the Library building will be established as a minimal backup computer facility.
- If it appears recovery of individual services will take longer than a week to restore, on a selective basis, services will be evaluated for possible out-sourcing to commercial organizations.

7.1.3 Preventive Measures

The Computer Services area and Central Computer Room are the two most important IT resources on the campus. Restoring this facility will be both expensive and time consuming. The current facility/room should be “hardened” to protect it from possible environmental or manmade damage. The following recommendations are made to protect this significant resource:

- Install a building and computer room alarm and monitoring system – both environmental, motion, and video, with a remote-notification capability.
- Develop and document a power plan for the central computer room.
- Replace older UPSs and put all UPSs on a standard replacement cycle.
- Protect the fiber optic and telecom cable entry point via a physical barrier.
- Provide better physical security for MDFs and wiring closets to preclude inadvertent or intentional damage.
- Contact possible offsite service providers (commercial and educational) who could, on an interim basis, host critical campus services.

7.2. Level 2 - GC Telecommunications

7.2.1 General

Grayson College provides internal and external phone service through a Voice Over IP (VoIP) telephone network used within the college network. Use of a VoIP saves the College from having to connect all of its telephone sets, separately, to the public telephone network, by using our internal, IP based, campus network. The GC VoIP network, is a cloud hosted system. GCEC is our telecom provider. All phone systems operate via SIP and transit the Internet to the cloud based hosting service. Even if the college experiences a catastrophic loss, our phone system will continue to operate, allowing customers to leave voice mail, or to directly contact any user, if the line has been forwarded to a working number, be it traditional landline or cell phone. This means the system can be accessed remotely, for answering calls, or checking voice mails, even if the college IP network is inoperable at our site. We can setup communications at a new location, off-site, as long as there is Internet access, with our existing handsets.

In addition to basic telephone services, campus voice mail, fax servers, and call accounting services are also provided by GCEC Telecommunications. GCEC uses a cloud based system, with redundant servers, hosted at a weather hardened, secure site.

There are several special circuits that the VOIP utilizes to provide telecommunication related services:

- There are four Internet Service Providers providing Internet connectivity to GC. Zayo Communications provides 1Gbit symmetric bandwidth. GCEC provides 400Mbit symmetric

bandwidth, TPX Communications provides 500Mbit symmetric bandwidth, and NETNET provides 100Mbit symmetric bandwidth. Any of which can be used for our SIP phones to access the remotely hosted VoIP service

7.2.2 Risk Assessment

7.2.2.2 Environmental Risk

- See paragraph 7.1.1.2, Environment Risks for Computer Services Area and Central Computing Room.
- VoIP's are designed to function in a wide variety of environments with a temperature range of 41F to 104F being acceptable.

7.2.2.3 Internal Systems Risk

7.2.2.4 External System Risk

- The VoIP utilizes our Internet circuits to provide connectivity to external phone systems
- 7.2.3 Recovery Planning
- In most situations, VOIP problems will be related to internal hardware problems. These problems usually affect only a few subscribers or pose an inconvenience and they are normally repaired by the Grayson College telephone technician, or a GCEC representative.
- In cases where hardware replacement is needed, GCEC can have the necessary part on site within 8 hours.
- If the GC on-site technician is unavailable, the help desk can be contacted via the online service request.
- In the case of a catastrophic failure of the VoIP network, impact to the campus would be severe and all phone and associated phone services would cease to function. In the event of a total system failure, GCEC communications support would be contacted and arrangements would be made to have all calls forwarded to another site, to be set up, and made operational by a team of technicians. This team most likely would respond within 2 to 8 hours from the North Texas area.

7.2.4 Preventative Measures

Refer to the preventive measures called out for Computer Services Area and Central Computer Room (paragraph 7.1.3).

In-place preventive measures include:

- Maintaining an inventory of PolyCom handsets on-site.
- Maintaining a certified GC VOIP technician.

Additional preventive measures, to be considered, should include the following:

- Installation of a fire suppression system in the central computer room.
- Creating a crash kit with spare parts, such as digital or analog trunk cards to minimize VoIP downtime, due to Internet loss.

- Develop a campus emergency communication strategy that assumes the VoIP is inoperable. This strategy should consider providing cellular phones to key GC personnel or departments and consider the use of instant messaging as an internal campus communication option.

7.3. Level 2 - GC 911 Emergency Services

7.3.1 General

Grayson College provides 911 and enhanced (E911) services through GCEC hosted phone services. The 911 system is dependent upon the VoIP to function. The primary 911 reporting unit is located at the GCEC hosting site. The 911 system provides two functions; the first is a stand-alone emergency reporting system for the college. The second function acts in tandem by reporting 911 calls to the local city emergency center. The enhanced 911 service provides a physical location for emergency for 911 calls. This physical address is stored in a data base within the hosted 911 system and in a second database maintained at an external AT&T site. The 911 database is maintained by the GC telecommunications technician and provided to GCEC for input into the E911 system.

7.3.2 Risk Assessment

7.3.2.1 Physical/Security Risk

- See paragraph 7.1.1.1, physical/Security Risks for the Computer Services Area and Central Computing Room.

7.3.2.2 Environmental Risk

- See paragraph 7.1.1.2, Environment Risks for Computer Services Area and Central Computing Room.

7.3.2.3 Internal Systems Risk

- The 911 system operates from the cloud based, remote hosting site operated by GCEC.
- The local 911 system operates off of POE (Power Over Ethernet) provided through a POE switch which operates off normal grid power, enhanced by a UPS. During a power outage, the 911 system will operate off of a backup battery system. Computer Services has a stand by generator that provides electrical power during grid power outages; consequently, electrical concerns are minimal. In the event of an electrical disaster, with the backup generator and backup battery system there would be little or no impact.

7.3.2.4 External System Risk

- The 911 system utilizes four ISPs to provide connectivity to external phone systems. If all four ISPs are down, or if there is multiple equipment failures to all four providers, GC's capability to make 911 calls will be impacted. As these circuits are maintained and serviced by multiple providers (Zayo, GCEC, TPX, NETNET), it will be the responsibility of the providers for the repair and restoration of service.
- If there is an external failure of all four of the providers, the E911 system will fail to function.

7.3.3 Recovery Planning

- In most situations, 911 system problems will be related to internal hardware problems. These problems are normally repaired by the Grayson College telephone technician. Assistance is also available from GCEC at 903.482.7000.
- In cases where hardware replacement is needed, the GCEC help desk can be contacted at 903.482.7000. This information is also posted on the front of the 911 system for quick reference.

7.3.4 Preventative Measures

- Refer to the preventive measures for Computing Services Area and Central Computer Room (paragraph 7.1.3).

Current preventive measures include:

- Maintaining an annual Shared Maintenance Agreement with 3Com Communications.
- Maintaining a certified GC VOIP technician.

Other preventive measures to be considered include the following:

- Installation of a fire suppression system in the central computer room

7.4 Level 2 – Network Infrastructure and Services

7.4.1 General

Network services are provided via the wired and wireless network infrastructure. Network services include a wide variety of functions, such as network/file storage (including the associated backup), printing, routing, switching, DNS and DHCP services, web/internet services, bandwidth allocation and monitoring, firewalls, etc. Network services are totally dependent on the campus cable plant and a wide variety of other commercial equipment including servers, switches, routers, wireless access points. Loss of network services impacts all other IT services.

7.4.2 Risk Assessment

7.4.2.1 Physical/Security Risk

- With the exception of the cable plant infrastructure and switching electronics located in the campus wiring closets and individual building main distribution facilities (MDF's), all other equipment supporting network services is located in the Central Computing room located in the Computer Services area. See paragraph 7.1.1.1 Physical/Security Risks for the Computer Services Area and Central Computing Room.
- There is currently one offsite network data storage capability. Though selected data is backed up to tape and stored offsite, data located on any disc backup system (web) would be lost if the Computing Services Computer Room was rendered inoperable.
- Telephone and data switching electronics are located in main distribution facilities (MDFs) and/or wiring closets located in each of the major campus buildings. Though each closet is

locked, in many cases, particularly in the residence halls, these closets are also used for miscellaneous storage and are accessed by other than Computing Services personnel.

- The risk for inadvertent damage and possible malicious damage is medium to high in these areas. Many closet environments are excessively dusty/dirty and suffer from significant humidity and temperature fluctuations. This can cause a higher than normal network electronic failure rate and reduce the lifetime of the copper network and telephone terminations/cabling.
- Network printers, PCs, and other devices are occasionally located in unsecured areas leaving them vulnerable to theft and vandalism.

7.4.2.2 Environmental Risk

- See paragraph 7.1.1.2, Environment Risks for Computer Services Area and Central Computing Room.
- Wiring closets/MDF's are not environmentally controlled and subject the equipment to varying humidity and temperature extremes and exposure to excessive dirt and dust. There is a risk of equipment and cabling failure because of the lack of a reasonable operating environment.

7.4.2.3 Internal Systems Risk

- Hardware or software failure impacting individual network services is a significant risk.
- Most network services do not have redundant hardware or fail-over systems in place. There are numerous unique hardware items that represent potential single points of failure.
- Equipment is used beyond its advertised/supported life due to budgetary constraints. Failed equipment will be replaced by spare, older, equipment obtained during equipment upgrade cycles.
- Adequate training and career growth opportunities must be provided to maintain GC's current network technical staff.
- Systems documentation, OS and configuration backup procedures, and training for backup personnel is accomplished on an ad hoc basis, resulting in differing levels of available documentation and competently trained personnel in the event of a major incident.
- All network equipment configurations are backed up weekly to a local desktop machine.
- Without establishing appropriate individual and group directory quotas, network storage availability could be exceeded, preventing any additional storage from occurring.
- Directory tree corruption could potentially require manual reinstallation of all network printer information for each individual device.

7.4.2.4 External System Risk

- Campus Internet connectivity is dependent upon one 23Ghz wireless system maintained by GCEC. This pathway can be damaged, resulting in the loss of external campus connectivity.
- Remote campuses in Van Alstyne receive Internet connectivity through one fiber optic line maintained by GCEC, with a failover bonded T1 link for phones provided by AT&T.

- There are currently no secondary (backup) data trunking pathways between campus buildings. If current cable plant pathways are damaged, network services will be impacted.
- Hackers could attempt to launch denial of service attacks and/or attacks against network equipment and IOS and/or configuration files.

7.4.3 Recovery Planning

Given the wide-variety of potential problems which could impact network services, the following generic recovery planning steps will be utilized to identify and resolve network problems:

- Assess which network service or services have been lost.
- Notify the campus, by whatever means available as to the service outage.
- Trouble-shoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support (see Appendix B for vendor contact information).
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

7.4.4 Preventative Measures

- Refer to the preventive measures for Computer Services Area and Central Computer Room (paragraph 7.1.3).
- Maintenance agreements are maintained on all critical servers and systems to help mitigate the lack of redundancy and to ensure rapid vendor response to problems. See Attachment C for a listing of vendor contacts and Attachment D for a server inventory.

Recommended preventive measures include:

- Establish a network refresh program to replace aging network equipment on a regular basis.
- Ensure that annual vendor maintenance agreements are in-place for all critical network systems.
- Maintain a pool of harvested, functional spares to provide replacement of failed, obsolete and un-repairable network switches.
- Procure backup hardware for critical, single point of failure systems.
- Work with the local community to establish a redundant fiber optic pathway.
- Develop a secondary campus core server and switching/routing plant with redundant connection to major building wiring closets.
- Develop and implement a plan for offsite storage/backup of major OS and configuration files.
- Provide more well-defined career growth opportunities for the network staff.
- Provide adequate training opportunities for the network staff to ensure technical proficiency in assigned areas of responsibility.
- Ensure that backup personnel are assigned for each critical network service.

- Provide adequate training to backup personnel on use of recovery procedures for network services.
- Buildup and maintain a stock of wiring closet hardware.
- Improve and standardize backup power to switches located in wiring closets.
- Where possible, do not use wiring closets for storage purposes.
- Where not possible, build locked cages around wiring closet electronics.
- Standardize wiring closet access.
- Improve climate control in wiring closets where there are significant temperature fluctuations.
- Relocate priority printing devices from vulnerable areas to more secure physical locations.

7.5 Level 2 - Cable Plant

7.5.1 General

The cable plant is a complex integration of copper wire and fiber optics. The cable plant is, in essence, the nerve system for campus communications. The cable plant provides the connectivity and communication paths for campus telephone and network users. The campus cable plant contains that is installed underground and within each of the campus buildings. The management focal point for the cable plant system is the Computer Services Central Computer Room, from which point it branches out all over campus.

7.5.2 Risk Assessment

7.5.2.1 Physical/Security Risk

- See paragraph 7.1.1.1 physical/Security Risks for the Computer Services Area and Central Computing Room.
- The cable plant is subject to damage from vandalism and unintentional damage caused by construction projects. Unintentional damage is the most common physical/security risk to the cable plant.

7.5.2.2 Environmental Risk

- The cable plant is subject to the effects of extreme temperature ranges and moisture. Over time, environmental conditions such as temperature and moisture will affect the reliability and quality of the cable plant.

7.5.2.3 Internal System Risk

- The cable plant was designed and engineered to conform to TIA/EIA industry standards to reduce the risk of installation damage and to ensure the required quality of service. Once installed, there is a minimal risk of component failure.
- The fiber optic portion of the cable plant is terminated at only a single location –Computer Services.

7.5.2.4 External System Risk

- Fiber optic and copper pathways that connect the GC cable plant with the AT&T data and phone infrastructure can and have been damaged, inadvertently. When this occurs, external network services will be impacted, until AT&T is able to repair its lines.

7.5.3 Recovery Planning

- In most situations when a cable or fiber optic is damaged on campus, the repair can be effected by personnel on staff.
- If damage occurs to off campus cables, the repairs have to be made by AT&T.

7.5.4 Preventive Measures

- Current preventive measures include properly installing copper wire and fiber optics in the proper pathways and in accordance with TIA/EIA standards.
- Periodical inspections of communication closets, pathways and vaults will help to eliminate potential problems.
- Cable damage from construction equipment could be reduced if construction plans were routed through Computing Services for review and approval.
- Controlled access to communication closets will reduce the probability of inadvertent storage-related damage and damage from vandalism.
- A reserve of emergency parts should be maintained to repair most anticipated types of damage.

7.6 Level 3 – File and Print Services

7.6.1 General

GC uses Microsoft Windows servers and UNIX based servers to provide campus file and print services. These servers provide campus computer users networked disk space to store files in personal home directories and collaborative group directories. Documents, spreadsheets, databases, and other digital information and programs store and retrieve data from these servers. Additionally, GC utilizes a third party print management system in open computer labs for easy and convenient self-serve payment and release options.

7.6.2 Risk Assessment

This risk assessment will deal only with the Microsoft Windows and UNIX based hardware, software and major dependencies required for proper operation of the Microsoft Windows and UNIX based File and Print Services systems.

7.6.2.1 Physical/Security Risk

All Microsoft Windows and UNIX based servers are located in the Computer Services Central Computing Room. Reference Paragraph 8.1.2, Central Computer Room Risk Assessment, for a description of the physical, environmental, electrical, external and internal risks associated with this location.

7.6.2.2 Internal Risk Assessment

- GC pays an annual maintenance licensing fees for all of the utilized Microsoft Windows and UNIX based software products. In the event application software is lost due to equipment malfunctions, all required application and operating system software could be obtained from the vendor, copied compact disks, or completely restored from Veeam Backup Images
- Periodically, a complete restore of the databases and selected directories are made to a test environment to ensure images and restore processes are current.
- All current production servers are covered under a basic Dell next day hardware warranty.

The most significant software-related risk is that associated with losing institutional data stored on Microsoft Windows and UNIX based file servers. To mitigate this risk, the following backup approach is currently in place to support Microsoft Windows and UNIX based disaster recovery needs:

- GC has migrated all production servers to a virtual environment. There are 2 hosts on the main campus that are mirrored so that in the event one fails the other takes its place.
- All servers are backed up locally on a dedicated VEEAM backup server. This server in turn uploads those backups as copies to iLand cloud service.
- In addition, there is a Hyper-V host and Domain Controller at the South Campus in Van Alstyne that could be used to get resources up and running again in the event of a catastrophic loss on the main campus.

7.6.2.3 External Risk Assessment

- Network connectivity is vital to the functionality of the Microsoft Windows and UNIX based servers. Microsoft Windows and UNIX based File and Print Services cannot operate without a functioning network.

7.6.3 Recovery Planning

- Assess which Microsoft Windows and UNIX based service or services have been lost.
- Notify the campus as to the service outage.
- Trouble-shoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

7.6.4 Preventive Measures

Refer to the preventive measures for Computer Services Area and Central Computer Room (paragraph 7.1.3). Current preventative measures include:

- Maintenance contracts are maintained on all Microsoft Windows and UNIX based hardware during the operational life of the equipment.
- Hardware and software patches and upgrades are installed on a regular basis.
- Novell data backup is performed on a regular basis.

- Review server clustering/high availability options to provide automatic failover and system redundancy in the event of hardware failure.

7.7 Level 3 –Enterprise Resource Planning (ERP) Services

7.7.1 General

The CAMS ERP system provides Grayson College with administrative information such as student finances, student records, payroll and benefit information, and provides a framework for self-service products that are available through the campus portal. This system serves almost all administrative staff on campus and also the on-campus student population and off-campus student population.

Integrated with CAMS is the Data Warehouse which relies heavily on the CAMS service being available. The CAMS system currently runs on an SQL Server, using a Windows Server 2012 R2 Operating System.

7.7.2 Risk Assessment

- This risk assessment will deal only with the CAMS hardware, software and major dependencies required for proper operation of the CAMS system.

7.7.2.1 Internal System Risk

- The most significant software-related risk is that associated with losing institutional data stored in CAMS's database. This risk has three components, which span both internal and external risks, including:
 - Internal database corruption which makes some or all of the data inaccessible.
 - Unauthorized personnel access to the CAMS system through malicious intrusion/hacking.
 - Unauthorized access to CAMS data through theft of data, such as theft of a laptop computer containing CAMS data.
- CAMS software and associated commercial software, as they are periodically updated, are all subject to software discrepancies, bugs and other associated problems.
- Adequate training and career growth opportunities must be provided to maintain GC's current CAMS programming and DBA staff.

7.7.2.2 External System Risk

- Network connectivity is vital to the functionality of the CAMS DBS. CAMS cannot operate without a functioning network.
- Unauthorized access to the CAMS data base via malicious hacking/intrusion to obtain sensitive personnel data is a significant risk.
- Loss of CAMS data through laptop or other theft is a significant risk.

7.7.3 Recovery Planning

- Initiate the *Grayson College Incident Response Plan* and Team
- Assess which CAMS service or services have been lost.

- Notify the campus as to the service outage.
- Trouble-shoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support, i.e. Unit 4 for the CAMS software and 3D Technologies LLC for the CAMS hardware.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

7.7.4 Preventive Measures

- CAMS system is backed up nightly. These backups are sent to the cloud storage services using Veeam, as well as stored locally, and lastly stored remotely with our hosting provider.
- GC pays an annual maintenance fee for all of the utilized CAMS software products and associated software products. As software bugs are identified, Unit 4 is notified. In the event application software is lost due to equipment malfunctions, all required application and operating system software could be obtained from the vendor or via backups.
- VPN Access is required to reach CAMS outside of the local network.

7.8 Level 3 - Email Services

7.8.1 General

Email services include email delivery, virus scanning, spam blocking, and email storage. GC utilizes Google G Suite for Education for core services including GMAIL, Calendar, Chrome Sync, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts, and Vault. Google offers these services for free to educational institutions, it's cloud based, available anywhere, integrates with our Active Directory for user management, and gives us SPAM/Malware protection and levels of control that would be cost prohibitive in an on-site, locally managed, solution. Google Vault also allows us to retain email for a specified period of time for legal purposes. This feature is also free.

7.8.2 Risk Assessment

7.8.2.2 Internal System Risk

- Internal system risks include software viruses and spam spread either intentionally or unintentionally throughout the network; viruses in particular can render the network unusable.
- Viruses: the vast majority of current viruses are transmitted via email. Viruses cause a reduction in productivity on workstations, and frequently require a Computer Services technician to clean or reclone the computer.
 - Incoming spam: some estimates place unwanted email (spam) at 90% of all email traffic. This has a significant impact on the user's productivity. Further, spam can introduce viruses and/or spyware onto a user's workstation.

- Outgoing spam: if the GC network is used to relay spam out to the Internet, our systems will likely be blacklisted, preventing our users from sending legitimate messages to their contacts.

7.8.2.3 External System Risk

On-campus email services are dependent upon the network/cable plant for continued operation. This includes fiber controlled by GCEC. Email services are web-based however and would still be available, outside our network, 24/7.

7.8.3 Recovery Planning

General Recovery Steps

- Assess which network service or services have been lost.
- Notify the campus, by whatever means are available, as to the service outage.
- Trouble-shoot to isolate the cause of the service outage.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.
- In the case of a major virus infection, ensure that campus virus protection software is updated and establish a Computing Services team to clean infected campus computers.
-

7.8.4 Preventive Measures

Physical access to the server(s)

- Preventative Measures: The door to the server room is kept locked.
- Action Items: Ensure that the college's cleaning crew and other, non-Computer Services staff, do not have access to the server room or ensure that those that do have access are properly educated about the security concerns. Better control of the back room by the front desk to ensure that visitors cannot walk around Computing Services freely.

Viruses

- Preventative Measures: GC uses Google to filter email for SPAM and MALWARE, though some items do get through, desktop preventative measures such as Windows Defender generally catch those items.
- Action Items: none.

Incoming spam

- Preventative Measures: GC uses Google to filter email for SPAM and MALWARE, though some items do get through, desktop preventative measures such as Windows Defender generally catch those items.
- Action Items: none.
- .

Outgoing spam

- Preventative Measures: GC is currently only allowing email relaying from certain IPs in its own IP address blocks. This prevents a remote spammer from using GC's mail servers directly.

Action Items: None

7.9 GC Web Services

7.9.1 General

- Grayson.edu provides GC's web presence including the Student and Community Portal.
- GC provides database back ends for web services, runs the content management system, and serves a read only replica of our LDAP directory.

7.9.2 Risk assessment

7.9.2.1 Internal System Risk

- Access to services authenticated by the Single Sign On service.
- Since there currently is no definition of acceptable downtime for these services, GC relies on a manual disaster recovery process (i.e. server rebuild).
- Software bugs and hardware failure are the primary internal system risks to the Web services area.

7.9.2.2 External System Risk

- Campus web services are dependent upon the network/cable plant for continued operation. This includes the 23Ghz wireless controlled by GCEC.
- GC web services could be compromised by hackers via web application exploits.

7.9.3 Preventative Measures

Current preventive measures include:

- GC relies on onsite backups, error logs, regular security updates, and security tripwire software for mitigation.
- Regular server and software security patching is performed to minimize the risk of unauthorized intrusion and/or exploitation.
- The main GC firewall is configured to block unnecessary external access to campus web servers.
- The server is a virtual machine housed on our local SAN, backed up daily, via Veeam, first locally, then via iLand to cloud storage.

Future preventive measures:

- GC uses AD and SAML authentication database. Access to Canvas and CAMS Web is not reliant on the Portal, alleviating the effects of any GC or Portal downtime.

7.9.4 Recovery Plan

- Recovery requires adapting to the specific disaster which has occurred. The following general recovery scenario is provided, which can be tailored, as necessary.
- General Recovery Steps:
- Assess which network service or services have been lost.
- Notify the campus, by whatever means are available, as to the service outage.
- Trouble-shoot to isolate the cause of the service outage.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

7.10 Level 3 – Campus Card Services

7.10.1 General

GC uses the Student ID Card System for campus card services. This system provides identification and limited debit-card services for students. The card is used in the campus cafeteria and other locations for vending, and provides door access to the gymnasium. The Student ID Card system was purchased in 2009 with new server hardware, operating system, management utilities, and selected campus hardware. Loss of Student ID Card impacts door access to the gym, meal plan vending, and miscellaneous other non-cash vending.

7.10.2 Risk Assessment

7.10.2.1 Physical/Security Risk

- The Student ID Card server is located in the Computer Services Central Computer Room and the two card terminals are located in the cafeteria in the Student Life building.
- ID Card hardware located in the Central Computer Room is secure and environmentally protected.
- ID Card hardware located in the Student Life building is environmentally protected and behind locked doors.

7.10.2.2 Internal System Risk

- A packet filtering firewall is utilized to limit external connectivity vulnerabilities.
- User passwords are changed on a regular basis.

- The ID Card software is relatively stable and problem free; there are periodic updates, as with all software.
- ID Card backups are performed on a daily basis.
- Given the significant monetary investment in the ID Card System, switching vendors would be a major challenge. This limits GC's flexibility in pursuing lower cost maintenance alternatives, mixing and matching hardware, etc.

7.10.2.3 External System Risk

- ID Card is dependent upon the network/cable plant for continued operation.

7.10.3 Recovery Planning

Depending on the scope and logistics of recovery, priority items would include:

- Server rebuild or replacement.
- ID Card database repair, recovery, or reinstall from backups.
- Network Manager(s) rebuild or replacement including proprietary cards installed.
- Campus ID Card Office Photo ID Services rebuild or replacement.
- Food Court Point of Sale equipment rebuild or replacement.
- Door controller(s) repair or replacement.
- Other End-point repair or replacement.

7.10.4 Preventive Measures

- Supplement the major single point of failure equipment. This includes: server, card printer and card encoder.
- A redundant, perpetual backup of database would help lessen problem of any lost transactions that have occurred between an existing backup and loss of primary database.
- There needs to be a periodic review of Campus ID Card administrative accounts and administrative terminals, combined with a policy of password change requirements.

7.11 Level 3 - Service: Residential Computing Services (ResNet)

7.11.1 General

Computer Services provides phone and direct technical support for students living on campus accessing the Internet using our wired and wireless network. If ResNet Services becomes unavailable due to a disaster, all on-campus students would lose their ability to access the Internet from their residence halls.

7.11.2 Risk assessment

7.11.2.1 Internal System Risk

Items of concern:

- Router controlling wireless access points could fail

CCA7.11.2.2 External System Risk

ResNet services are dependent upon the network/cable plant for continued operation. This includes fiber controlled by AT&T Communications.

7.11.3 Preventative Measures

Multiple access points throughout campus provide safety net in case of a single failure. Back up router available to replace failed router.

7.11.4 Recovery Plan

General Recovery Steps:

- Assess which network service or services have been lost.
- Notify the campus, by whatever means are available, as to the service outage.
- Trouble-shoot to isolate the cause of the service outage.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

7.12 Level 3 - Academic Instructional Technology Classrooms

7.12.1 General

Instructional technology classrooms fall into two categories. These include Technology Enhanced Classrooms (TECs) that normally contain an instructor computer, projector, sound system, and document imager and Dual Purpose Student Computer Laboratories in which classes are also taught.

7.12.2 Risk Assessment

- The IT services necessary to support technology enhanced classrooms are covered in other areas of this document and include items such as: cable plant, network, email, and Canvas. Once these basic services are restored most IT-dependent classes can continue.

7.12.2.1 Internal System Risk

- Computer hardware and peripherals are subject to normal, random component failures.

7.12.2.3 External System Risk

- Academic TECs are highly dependent upon the IT connectivity provided by Computer Services through the campus cable plant. Network classroom equipment is susceptible to theft and malicious damage. The academic buildings do not have backup power. All classroom IT equipment uses commercial power and is subject to periodic power outages and power fluctuations.

7.12.3 Recovery Planning

- In the event of the loss of a Technology Enhanced Classroom or building to the level constituting a disaster, classes will be rescheduled in other TECs across campus.
- Reconstruction of the TECs will be prioritized along with other IT components impacted by the disaster.

7.12.4 Preventive Measures

Current Preventive Measures:

- Computer Services has established an equipment refresh schedule for the approved TECs. This provides a reasonable equipment replacement cycle and the ability to develop, over time, a spares pool consisting of the replaced hardware.
- A limited stock of spare equipment is maintained by Computer Services to provide a swap out capability.
- Computer Services is striving to make each TEC identical, in terms of IT equipment, to simplify the hardware repair and replacement process.
- Computers are re-cloned on a periodic basis to bring the software operating systems and applications back to an original state, removing any miscellaneous programs that may have been installed by student users.

Recommended Preventive Measures:

Any academic area which has a unique IT service that is not addressed elsewhere in this document, must list the service with Computer Services to ensure it can be prioritized in the event of a disaster. For non-disastrous equipment failures or network outages, instructors should have alternative lesson plans and backup material available.

7.13 Level 3 – Student Computer Lab Services

7.13.1 General

GC provides more than 20 student computer laboratories, containing more than 350 desktop computers. Student computer laboratories are located in every major academic building including the the South Campus in Van Alstyne and the GC West Campus.

7.13.2 Risk Assessment

- The IT services necessary to support student computer labs are covered in other areas of this disaster plan and include items such as: network infrastructure, email, CAMS portal, and Canvas. Once these basic services are restored most IT-dependent classes can continue.

7.13.2.1 Internal System Risk

Computer hardware and peripherals are subject to normal, random component failures.

7.13.2.2 External System Risk

- Student computer labs are highly dependent upon the IT connectivity provided by Computer Services through the campus cable plant and network.

- Student computer lab equipment is susceptible to theft and malicious damage.
- The academic buildings do not have backup power. All student computer lab equipment uses commercial power and is subject to periodic power outages and power fluctuations.

7.13.3 Recovery Planning

In the event of the loss of a student computer lab or building to the level constituting a disaster, student computer labs in other academic buildings will be available to support campus needs.

Reconstruction of the student computer labs will be prioritized along with other IT components impacted by the disaster.

7.13.4 Preventive Measures

- Current Preventive Measures:
- Computer Services has established an equipment refresh schedule for the approved student computer laboratories. This provides a reasonable equipment replacement cycle and the ability to develop, overtime, a spare parts pool consisting of the replaced hardware.
- A limited stock of spare equipment is maintained by Computer Services to provide a swap out capability.
- Computer Services is striving to make each student computer lab identical, in terms of IT equipment, to simplify the hardware repair and replacement process.
- Computers are re-cloned on a periodic basis to bring the software operating systems and applications back to an original state, removing any miscellaneous programs that may have been installed by student users.
- Most desktop computers in the student labs contain Clean Slate, a security program designed to restore the computer system back to its original state after a reboot.

8.0 MAINTENANCE OF THE IT DISASTER RECOVERY PLAN

The effectiveness of this disaster recovery plan is impacted by changes in the environment that the plan was created to protect. Some major factors, which will impact the plan, are new equipment, changing software environment, staff and organizational changes, and new or changing applications.

Annually, the Vice President of Information Technology will ensure that the document is reviewed and updated (if required) by a team of Computer Services personnel. This review will include an assessment and update of recommended action items found in Appendix A.

9.0 APPENDICES

Appendix A: IT Disaster Recovery Plan Action Items

Appendix B: Vendor Contact Information

**Appendix A
Possible Action Items**

Item #	Status	Comments
1.	7.1 Computer Services (CS) Area and Central Computer Room	Install a building and computer room alarm and monitoring system – both environmental, motion and video, with a remote-notification capability
2.	7.1 Computer Services (CS) Area and Central Computer Room	Construct a pitched roof to protect the computer room from possible water damage from rain or melting snow.
3.	7.1 Computer Services (CS) Area and Central Computer Room	Designate additional storage areas outside of the CS area to reduce building clutter and reduce the amount of flammable material on-hand.
4.	7.1 Computer Services (CS) Area and Central Computer Room	Develop and document a “power” plan for the central computer room.
5.	7.1 Computer Services (CS) Area and Central Computer Room	Re-wire the backup air conditioner to allow generator operation for both air conditioners.
6.	7.1 Computer Services (CS) Area and Central Computer Room	Replace older UPSs and put all UPSs on a standard replacement cycle to ensure a seamless cutover to generator power, if and when, there are power failures.
7.	7.1 Computer Services (CS) Area and Central Computer Room	Provide better physical security for MDFs and wiring closets to preclude inadvertent or intentional damage.
8.	7.1 Computer Services (CS) Area and Central Computer Room	Establish a standby computer room on the 1st floor of the LA building.
9.	7.1 Computer Services (CS) Area and Central Computer Room	Contact possible offsite service providers (commercial and educational) who could, on an interim basis, host critical campus services.
10.	7.2 Telecommunications	Creating a crash kit with spare parts, such as digital or analog trunk cards to minimize VOIP downtime.
11.	7.2 Telecommunications	Develop a campus emergency communication strategy that assumes the VOIP is inoperable.

Item #	Status	Comments
12.	7.2 Telecommunications	Maintain a spare server that will run the voice mail operating system.
13.	7.4 Network Infrastructure & Services	Establish a network refresh program to replace aging network equipment on a regular basis.
14.	7.4 Network Infrastructure & Services	Ensure that annual vendor maintenance agreements are in-place for all critical network systems.
15.	7.4 Network Infrastructure & Services	Maintain a pool of functional spares for equipment replacement.
16.	7.4 Network Infrastructure & Services	Ensure that backup personnel are assigned for each critical network service.
17.	47.4 Network Infrastructure & Services	Provide adequate training to backup personnel on use of recovery procedures for network services.
18.	7.4 Network Infrastructure & Services	Buildup and maintain a stock of wiring closet hardware.
19.	7.4 Network Infrastructure & Services	Improve and standardize backup power to switches located in wiring closets.
20.	7.4 Network Infrastructure & Services	Where possible, do not use wiring closets for storage purposes. Where not possible, build locked cages around wiring closet electronics.
21.	7.4 Network Infrastructure & Services	Standardize wiring closet access.
22.	7.4 Network Infrastructure & Services	Improve climate control in wiring closets where there are significant temperature fluctuations.
23.	7.4 Network Infrastructure & Services	Relocate priority printing devices from vulnerable areas to more secure physical locations.
24.	7.4 Network Infrastructure & Services	Procure backup hardware for critical, single point of failure, systems.
25.	7.4 Network Infrastructure & Services	Provide more well-defined career growth opportunities for the network staff.
26.	7.4 Network Infrastructure & Services	Provide adequate training opportunities for the network staff to ensure technical proficiency in assigned areas of responsibility.

Item #	Status	Comments
27.	7.5 Cable Plant	Periodically inspect the communication closets, pathways and vaults to help eliminate potential problems.
28.	7.5 Cable Plant	Cable damage from construction equipment could be reduced if construction plans were routed through Computer Services for review and approval.
29.	7.5 Cable Plant	Controlling access to communication closets will reduce the probability of inadvertent storage-related damage and damage from vandalism.
30.	7.5 Cable Plant	Maintain a reserve of emergency parts to repair the most anticipated types of damage.
31.	7.6 Network File & Print	Review clustering/high availability options to improve system availability.
32.	7.7 CAMS ERP System	Implement a more-frequent password change policy.
33.	7.7 CAMS ERP System	There is still the need to train personnel on the use of stronger and longer passwords to provide better security.
34.	7.8 Email	Possibly block outgoing SMTP connections originating anywhere other than our mail servers to prevent workstations, particularly those in the dorms, from sending spam.
35.	7.8 Email	Require users of standalone clients to use the encrypted protocols instead of the unencrypted ones. This may break functionality with PDAs, as they tend to have extremely limited functionality.
36.	7.9 Web Services	Since web backups are currently stored to disc and not on tape media, an offsite storage capability should be developed.

Item #	Status	Comments
37.	7.9 Web Services	GC has action items to configure Canvas and CAMS to use the AD and SAML authentication database. When that happens, access to Canvas and CAMS Web will not be reliant on the Portal, alleviating the effects of any Portal downtime.
38.	7.9 Web Services	Migrate to a new Operating System.
39.	7.10 ID card System	Supplement the major single point of failure ID card equipment. This includes: server, card printer and card encoder.
40.	7.10 ID card System	A redundant, perpetual backup of database would help lessen problems of any lost transactions that have occurred between an existing backup and loss of primary database.
41.	7.10 ID card System	There needs to be a periodic review of Campus ID Card administrative accounts and administrative terminals, combined with a policy of password change requirements.
42.	7.11 ResNet Services	Purchase additional Clean Access hardware to provide necessary system redundancy.
43.	7.11 ResNet Services	Send the CCA system administrator to vendor training.
44.	7.12 Tech Classrooms	Any academic area which has a unique IT service that is not addressed elsewhere in this document, must list the service with Computer Services to ensure it can be prioritized in the event of a disaster.
45.	7.12 Tech Classrooms	For non-disastrous equipment failures or network outages, instructors should have alternative lesson plans and backup material available.

**Appendix B
Vendor Contact Information**

3D Technologies LLC

817-385-7034

AT&T

Special Circuit and PRI Repair
800-442-9950

Voice Services Repair
800-286-8313

Axxys Technologies

903-893-6548

Cable One

903-893-6548

DIR

512-463-3449

Google

903-893-6548

GCEC

903-482-7000

Identity Automation

281-220-0021
support@idauto.net

Instructure (Canvas)

800-203-6755

NetNet

903-877-1258

Unit 4

636-779-1521
636-386-8616

Zayo

682-207-1145