A&GS IT Policies & Strategic Plan

November 24, 2014

Table of Contents

Version and Revision Log

Version	Approved Date	Approved by	Description of Change

IT Governance Program

Purpose

The purpose of this program is to provide a framework of IT governance, and define a IT strategy in alignment with the business objectives of the College of A&GS at the University of Oklahoma. The IT Governance Program applies to IT personnel and related assets in A&GS. IT Governance is an integral part of an organization that consists of leadership, organizational structures and processes that ensure the organization‘s strategies and objectives are sustained and extended by information technology.

Roles and Responsibilities

The A&GS Directors' Council (ADC) consists of the directors of all academic and research units in the College of A&GS. The ADC reports to the Dean of A&GS and is responsible for general oversight and support of the program. More specifically, the responsibility of this Council is to

- Define and review the IT governance structure, business model, value and mission, strategic IT objectives, long term and short term plans for A&GS in line with the IT requirements of the University of Oklahoma.
- Play an advisory role for critical IT decisions.
- Decide on significant IT investments, especially those costs that are shared across multiple units.
- Design and review the measurements of IT performance and ensure continuous improvement on performance metrics.

The IT Council consists of the system administrators and key IT staff in each unit of A&GS and is chaired by the Director/Senior Manager of RCS. The responsibility of this Council is to

- Establish IT management policies and mechanisms, set up implementation plans and performance measurement that support the strategic priorities.
- Define technical architecture and standard for the college, and establish best practices and tools for IT function across the college.
- Communicate with OU IT executive and professionals on the latest requirements on infrastructure, architecture and other technical considerations.
- Training and technical documentation related to information technology.
- The IT Council reports to the ADC. Each IT system administrator advises his or her unit head on specific IT issues within the unit and the College.

A&GS Strategic IT Plan

The A&GS Strategic IT Plan is to provide information technology services to facilitate education and research by enhancing communication and knowledge; proactively engaging on innovation and growth; collaborating with College faculty, staff and students to improve efficiency and reduce cost; planning for the future and cultivating relationships both inside and outside of our University.

IT Governance Policy

- Each unit in A&GS will review the strategic plan and assess its specific application and implementation within that unit.

- Each unit head will document and communicate expectations and commitments to his/her system administrator or key IT staff.
- The ADC and IT Council shall review this program annually to ensure it is applicable and in compliance with federal, state and University rules and regulations.
- The IT Council will communicate regularly with OU IT and keep up relations with other IT groups on campus and in the community.
- The IT Council will advise the ADC on industry trends, further the strategic objectives, and prioritize planned action items.
- Each unit will define and document a short and long term plan by discussion between the ADC and the IT Council. Any change to the plans shall be documented and must be approved by ADC.
- New projects will be evaluated by both the system administrator(s) and unit head. If the project is large scale or may impact other units, the proposal shall be submitted to the ADC for review and evaluation prior to implementation.

Short Term Plan

- Enhance the server inventory management system, and IT resource management in A&GS.
- Holistic backup solution including offsite system at alternate site
- Build a robust risk management and vulnerability monitoring mechanism.
- Promote awareness of all programs and policies by providing materials online in a shared environment. May establish an A&GS wiki, a Sharepoint space, etc.

Long Term Plan

- Conduct broader risk assessment for each unit.
- Conduct a business impact analysis for A&GS as a whole, not only IT specific.
- Globalization of teaching, learning, research, and outreach
- Further technologies for online learning in virtual environments
- Personalized learning and learner analytics
- Cloud services and research computing

Monitoring and Reporting Mechanism

The ADC and the IT Council have set up a performance appraisal mechanism for evaluating and monitoring the performance of IT in the college by focusing on the results of our IT audit, regular review of our IT Policies, IT staff turnover, customer satisfaction surveys, incident response statistics, down time and training provided to College personnel. The ADC and IT Council will meet annually to analyse the results of these measures and respond as needed.

Training and Documentation

Research Computing Services (RCS) will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources. RCS is responsible for oversight of each unit in A&GS to ensure IT policy compliance, and provide guidance and education.

Business Continuity and Disaster Recovery Program

Purpose

Information technology is vital to business processes in A&GS, and it is critical to establish a solid plan to recover systems and data efficiently and effectively following a service disruption. The Business Continuity and Disaster Recovery (BCDR) Program applies to the critical information systems resources in A&GS, including but not limited to all hardware, software, electronic data, and the personnel related to information technology. The BCDR Program covers all key administrative, personnel, and technical areas required for a business unit to recover from a disruptive event. OU IT involvement is heavy due to high dependence on OU IT resources.

Roles and Responsibilities

- **The A&GS Directors' Council (ADC)** is responsible for general oversight and support of the BCDR Program. A contact list of ADC members shall be maintained and accessible to all relevant individuals.
- **The IT Council** is responsible for the IT disaster recovery process. A contact list of IT Council members shall be maintained and accessible to all relevant individuals.
- Each unit may develop a complimentary plan to further develop this BCDR Program and customize it for their systems and environment.
- The ADC and the IT Council shall meet regularly for major decision-making. The IT Council shall report to the ADC regarding technical matters of the disaster recovery plan, and obtain approval for major decisions.
- Pertinent portions of the BCDR Program shall be posted on a public A&GS website to ensure each individual in A&GS has access to it. A printed copy will be available in both Dean's Offices in NWC 3630 and in SEC 510.

Business Impact Analysis (BIA)

- A&GS has performed a preliminary risk assessment to determine current system vulnerabilities and potential threats. The ADC and IT Council will review this annually to continuously improve the program.
- A&GS has performed a preliminary business impact analysis to document and understand the interdependencies among business processes to determine how they would be affected by an IT outage. The ADC and IT Council will update and review this annually to ensure its relevance and further develop the program.
- Based on the business impact analysis, the IT Council has identified single points of failure within the critical IT infrastructure, critical applications, systems and data, and prioritized key business functions in the recovery process.
- The staff relevant to the plan shall receive guidance and instruction regarding roles and responsibilities in the plan, and to keep them updated regarding any changes made to the plan.

Business Continuity Plan

- General contingencies: fire, flood, tornado, earthquake, and pandemic disease outbreak.
- Basic infrastructure contingencies: loss of power, loss of HVAC, loss of equipment, loss of connectivity, loss of space/facility.
- For other technical contingencies, like network service and other IT related services, RCS shall maintain a complete list of personnel, facilities, and technology (hardware, software, telecommunications, network and operational equipment) required for recovery operations. The contact lists include internal A&GS personnel and external vendors.
- RCS and each unit in A&GS shall ensure appropriate maintenance of vendor documents, and ensure that they are updated and accessible in the event of system outage.

Recovery Procedures

Activation and Notification Phase - Once disruption is detected or appears imminent, the ADC or the IT Council can activate the recovery procedures and all personnel shall be notified immediately. For purposes of planning and testing, we assume that OU still has power, network and space and only the National Weather Center is destroyed. The following should be notified using contact lists in Appendix:

- A&GS IT Council
- A&GS ADC
- A&GS College Personnel

The IT Council may initiate an outage assessment to determine the extent of the disruption and expected recovery time.

System administrators will begin immediately implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities.

Infrastructure services are primarily maintained by OU IT. Services such as DNS, DHCP, and OU Email should already be running at SEC (alternate site location). A&GS systems in NWC would need to be set up in SEC from backups. Some systems are already in place, some would need to be purchased.

Preventive Actions

- Backup Plan – RCS performs incremental backups every day and a full backup every 4 weeks. Copies of full backups are stored on tape and taken off-site every four weeks.
- UPS - OU Facilities Management with oversight from the National Weather Center IT Council shall ensure that the UPS systems in the NWC are provided with appropriate kilovolt amps of uninterruptible power for the critical services and process required.
- Facility Access - The NWC and SEC data centers are physically locked; only authorized personnel are given access with Sooner OneCards and NWC Keycards. The IT Council performs routine maintenance and monitoring of the facilities to identify and address potential issues. RCS keeps the data centers hazard-free and climate controlled. Other preventive measures exist such as a fire extinguishing system, smoke detectors, raised floors, and room monitoring hardware/software to detect and mitigate the chance of disaster. RoomAlert™ systems are installed in both data centers to notify IT staff about temperature and humidity problems.

IT Disaster Recovery Plan

- Alternative Site – In the event of a major disaster, A&GS will relocate to offices in Sarkeys Energy Center (SEC). The A&GS Dean retains office space there and will be able to support 10-12 people for a brief amount of time. The alternative site already has power, network and other needed resources. Many staff members will be able to telecommute from home or off campus. If any additional space is required, the Dean of A&GS will petition University of Oklahoma administration for alternative options.
- Training and Documentation - Research Computing Services (RCS) will ensure that all personnel in A&GS are provided with the A&GS IT Policies and will clearly define and communicate the roles and responsibilities in the event of a system outage.
- Communication in Contingency - Cell phones will be used as major communication tools in the event that voice and data services offered by OU and the National Weather Center are unavailable.

Testing Procedure

- Testing Plan – The IT Disaster Recovery Plan will be tested annually at the ADC and IT Council meeting to assess the effectiveness of the process. Each group will run through a hypothetical scenario and role-play the recovery steps.
- Test Notification - Prior to testing, notification shall be given to relevant individuals regarding the timing, schedule and possible system disruption during the testing.
- Results Analysis - Results from the testing shall be reviewed by the ADC and the IT Council, and discrepancies shall be assessed to come up with an improvement action.
- Documentation - The test process and results shall be well documented.

Review

- The BCDR plan shall be reviewed and analyzed on an ongoing basis to ensure alignment with the A&GS IT Strategic Plan and current business requirements.
- Research Computing Services (RCS) will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources. RCS is responsible for oversight of each unit in A&GS to ensure IT policy compliance, and provide guidance and education.

Appendix

- Business Impact Analysis
- Risk Assessment
- Personnel Contact Lists
- Vendor Contact List

Risk Management Program

Purpose

The purpose of this risk management program is to protect critical information resources in A&GS through thorough risk identification, assessment, response and monitoring mechanisms, and also enable A&GS directors to make well informed decisions on risk management.

Definition

- **Threats** are potential of a threat source to exploit a specific vulnerability. Threat sources can be both internal and external. Examples are hacking, acts of terrorism, unauthorized access, etc.
- **Vulnerabilities** are weakness or holes in information systems allowing the potential for unauthorized change or manipulation, impacting confidentiality, integrity and availability (CIA) of information systems.
- **Impacts** are the costs associated with failure in protecting the CIA of information systems.
- **Risk**: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby impact the organization.
- **IT Risk Assessment –** the process of weighing and prioritizing risk to IT asset.

Roles and Responsibilities

- **The IT Council** is the major responsible party for the risk management program. The IT Council shall meet annually to review both the documents and practice, and report to the A&GS Directors' Council (ADC) on the risk management plan.
- **The ADC** shall decide on the risk framework and play an oversight role on risk management.
- **Research Computing Services** (RCS) will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources.

Risk Assessment and Analysis

A&GS selected the NIST/FISMA framework for risk management. This Risk Management Framework (RMF) will be utilized for all A&GS IT systems and processes in the future. The IT systems administrators have begun the risk assessment process and will report to the ADC with results in 2015. RCS developed a Risk Assessment Checklist and a Risk Assessment Form for itemized analysis of systems. The risk assessment plan and documents shall be reviewed and evaluated annually.

FISMA RMF Steps

- **Step 1: Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- **Step 2: Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.
- **Step 3: Implement** the security controls and document how the controls are deployed within the information system and environment of operation.
- **Step 4: Assess** the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Step 5: Authorize** information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- **Step 6: Monitor** and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials.

Current Compliance

- The server inventory for both data centers is complete.
- We have established a Data Classification System and are applying it to current systems.
- The University of Oklahoma IT department (OU IT) performs regular network security scanning of the entire OU network environment to detect the system vulnerabilities. A&GS systems are scheduled for a network scan every 6 months. System administrators in A&GS are responsible for the security of local systems, physical computers and facility control.

Risk Response Procedure

With the risk identified and risk level determined in the risk assessment process, the IT Council will choose to avoid, mitigate, plan, transfer or accept the risks.

- **Avoid -** avoid risk by eliminating the risk cause or consequence.
- **Mitigate** - minimize the adverse impact of threat vulnerability by implementing controls, like detective tools.
- **Plan** - define priority and action plan to be taken in response to risks.
- **Transfer** - lower risks by using other options like purchased insurance.
- **Accept** – do nothing if cost-benefit considerations rule out alternative strategies.

Risk Monitoring Procedure

- The IT Council will monitor systems to verify whether the risk response measures are implemented and current security controls are in compliance with relevant rules and regulations, and to further evaluate the effectiveness of risk response measures.
- Automated tools have been put into place like the bi-annual OU IT Network Scan and the RoomAlert™ environmental system and sensors.
- The IT Council will meet regularly to evaluate the effectiveness and compliance of implementation of risk monitoring and modify the frequency of monitoring if needed.

Server Management Program

Purpose

This program establishes requirements and procedures for locating, installing, configuring, maintaining, patching and monitoring the integrity of A&GS servers, to ensure resource availability, information and assets security, and vulnerabilities mitigation. In A&GS, a server is defined as a computer system (software and hardware) that responds to requests across a computer network.

Roles and Responsibilities

- **The Unit Head** is responsible for ensuring compliance with A&GS policies and procedures, approving access to the server, and ensuring that a qualified system administrator is identified to manage the system
- **The System Administrator** is responsible for managing the hardware, networking, operating systems, and security of the server. The System Administrator shall be clearly designated and provided with proper training.
- **Research Computing Services (RCS)** will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources. RCS is responsible for oversight of each unit in A&GS to ensure IT policy compliance, and provide guidance and education.

Policy

1. Purchases - The system administrator must obtain the approval of the unit head or grant PI prior to purchasing server hardware / software, and after assessing business need and technical viability.
2. Server Inventory System - RCS maintains a centralized server inventory management system for all A&GS. All servers are located in designated rack spaces approved by RCS. A record of all servers and equipment is kept and updated regularly by each system administrator. Maintenance and updates of the inventory are conducted regularly, and this process is evaluated by RCS to ensure it continues to meet the security policies of A&GS.
3. Authentication and Password Protection - All accounts and password protection must be managed in accordance with all applicable policies and Access Management Procedures.
4. Remote Administration - All remote access to the server from off campus or outside of the NWC building shall utilize an approved Virtual Private Network (“VPN”).
5. Logs - All logs generated by A&GS servers shall be retained in accordance with the Privacy and Records Management Program.
6. Backup - The system administrator of each unit shall ensure that his/her unit has a documented backup plan, which is implemented as required in a timely manner in accordance with the Business Continuity and Disaster Recovery Program.
7. Security - The system administrator of each unit shall set up the security configuration and update the security package in a timely manner to mitigate any potential risks. An anti-malware application shall be installed on each server, where possible. The OU IT Security team has scheduled a regular scan of all servers to detect and eliminate malware every 6 months.

8. Vulnerability and Risk Assessment - Vulnerability scanning and risk assessment are performed on a regular basis on all servers; the impact analysis shall be renewed annually to evaluate the key risk factors, and those factors shall be addressed and resolved in accordance with the Risk Management Program.
9. Removal of Data - The system administrator of each unit shall ensure data is removed or emptied in accordance with the Privacy and Record Management Policy.
10. Configuration Management - The system administrator is responsible for establishing the appropriate baseline configuration of software and hardware for servers based on business requirements, security requirements and in accordance with the relevant policies. It is advised that the configuration follow industry best practice. RCS will play a consulting or advisory role when needed.
11. Change Control - The system administrator can approve or deny a change proposal, and when necessary, an impact analysis shall be conducted to ensure that the requested change is not incompatible with the original framework and will enhance the system integrity. When needed, the system administrator or unit head can submit the change request to the IT Council for advice.

Data Classification Program

In order to protect the confidentiality, integrity and availability of data, and prevent data from unauthorized generation, access, modification, disclosure or destruction, all personnel in A&GS shall be responsible for the implementation of this program.

Data owned, used, created and maintained by A&GS are classified into four categories.

1. Public
2. Sensitive
3. Restricted
4. Highly Restricted

Each unit shall carefully evaluate and define the classification of data based on the following criteria:

1. **Public Data** is information with no legal restrictions on access or usage, and shall be available to all members of A&GS and the public. It may be freely disseminated without potential harm to A&GS.

   Examples: advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases, instructions, training manuals.

2. **Sensitive Data** is information that is not openly shared with the general public but is not specifically required to be protected by statute, regulation, or by department, unit or A&GS policy. It is intended for use by a designated workgroup, department or unit within the University. Unauthorized disclosure of this information could adversely impact A&GS.

   Examples: budget and salary information, personal pager or cell phone numbers, departmental policies and procedures, internal memos, incomplete or unpublished research.

3. **Restricted Data** is highly confidential information. There are often general statutory, regulatory or contractual requirements that require protection of the data. It is intended for a very specific use and should not be disclosed except to those who have explicit authorization to review such data. Unauthorized disclosure of this information could have a serious adverse impact on A&GS and the University. Regulations and laws that affect data in DCL3 include, but are not limited to, Family Educational Rights & Privacy Act (FERPA) and the Graham-Leach-Bliley Act (GLBA).

Examples: Student data that is not designated directory information; other personally identifiable information (PII) such as name, birthdate, address, employee ID, etc. where the information is held in combination and could lead to identity theft or other misuse; certain research (e.g. proprietary or otherwise protected).

4. **Highly Restricted Data** is information that is required to be strictly protected. There are often governing statutes, regulations or standards with specific provisions that dictate how this type of data must be protected. It is intended for a very limited use and must not be disclosed except to those who have explicit authorization to view or use the data. Unauthorized disclosure of this information could have a serious adverse impact on A&GS and the University. Regulations, laws and standards that affect data in DCL4 include, but are not limited to, the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), the Export Administration Regulations (15 CFR 730 et seq.), the Health Insurance Portability & Accountability Act (HIPAA) and Payment Card Industry (PCI) standards.

   Examples: Biometric data, e-commerce, export controlled data, national security interest (NSI), protected health information (PHI), social security numbers (SSNs).

Data Ownership, Roles and Responsibilities

- Each system administrator with guidance from his/her respective unit head is responsible to define the classification of the currently available data for his/her unit, take appropriate security measures based on the data classification requirement, and set up the access level for each employee based on the roles and job description in accordance with the Access Management Program.
- RCS shall provide documentation and guidance on data classification and relevant security requirements; each unit shall promote security awareness within their own unit.
- RCS shall review and reevaluate the process annually for compliance with latest applicable regulations and the effectiveness of the process. Modifications and revisions shall be disseminated to all relevant individuals.

Review and Evaluation

The system administrator in each unit will regularly review and evaluate the configuration plan, specifications, and tools to ensure system weaknesses and vulnerabilities are detected, and the configurations are appropriate for the level of sensitivity/confidentiality required.

Software Application Management Program

Purpose

The purpose of this program is to provide guidance on software management in A&GS, and ensure security and information confidentiality, integrity and availability during each stage of development.

Definition

- **Software** – is defined as a set of instructions and statements that a computer uses to bring about a desired result. In A&GS, software can include operating systems, office software, graphics software, media viewers, security software, etc.
- **Commercial off the shelf** – software and hardware that already exit and are available from a commercial source.
- **System development life cycle (SDLC) -** is a term used in systems engineering, information systems and software engineering to describe a process for initiation, acquisition/development, implementation, operations/maintenance and disposition of information systems.
- **A Penetration Test -** is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to its functionality and data.

Responsibility

- **The System Administrator** of each unit shall play a key role in the implementation of this program and report results to the ADC.
- **The IT Council** plays an advisory role in the program and is responsible for reviewing the program at annually.

Policy

Software Acquisition/Procurement

- Software acquisition requests shall be assessed prior to procurement on the technical feasibility and the potential risks by the system administrator to ensure that the software incorporates adequate security controls for its intended purpose.
- After proper risk assessment, the unit head can approve or not approve the purchase based on budget considerations.
- Generally, software and license information are provided by OU IT and the OU IT Store. In the event that additional hardware or software is needed, OU IT resources shall be utilized and the purchase made through Crimson Corner where available.
- Software shall be patched as soon as possible to remove security vulnerabilities.

Software License

- Under no circumstances should unlicensed software be loaded onto any system in the A&GS. Software can only be installed and used in accordance with the license agreement.
- The system administrator of each unit is responsible for ensuring secure installation of the software, and for maintaining license compliance.

Software Development

- A&GS suggests the RAD or SDLC methodologies for software development, and require that developers incorporate industry best practice during each step of the cycle.
- Security and risk analysis shall be performed at each stage of development and tested before it is released to the production environment.
- A development environment shall be maintained and isolated from production environment.
- A source code repository shall be well maintained by the developer with restricted access control. Any major change request shall be reviewed and subject to approval by the system administrator.
- The IT Council is responsible for application incident response in accordance with the Business Continuity and Disaster Recovery Plan.

Security Management

- The system administrator is responsible for assessing whether user access to applications is authorized and in compliance with the Access Management Program, to ensure that application can be accessed only by authorized personnel.
- Configuration management of software shall be limited to system administrators in each unit in accordance with Server Management Program and Configuration Management Program.
- Third party access to applications or related information shall adhere to requirements in the Access Management Program.
- The management of confidential application information shall adhere to the data classification policy in the Server Management Program.
- The restoration of applications or data shall occur in accordance with Business Continuity and Disaster Recovery Program.

Log Management

The system administrator of each unit is responsible for managing the logs on each server; he/she will ensure they are maintained, protected, and analyzed in accordance with the Access Management Program.

Policy Approval and Management

The Software Management Program shall be reviewed by the IT Council annually, and approved by the ADC for implementation. Research Computing Services (RCS) will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources. RCS is responsible for oversight of each unit in A&GS to ensure IT policy compliance, and provide guidance and education.

Access Management Program

Purpose

The purpose of this policy is to define access control measures for systems, servers, applications and other shared IT resources in A&GS, to protect the confidentiality, integrity and availability of information systems and meet the privacy and security requirements.

Definition

- **Access** – the ability to use, modify or manipulate information and data or have physical entry to certain areas or functions.
- **Access Management** – The process of granting authorized users the right to use a service, while restricting access to non-authorized users.
- **Role-based Access Control (RBAC) -** In IT systems security, RBAC is an approach to restricting system access to authorized users. It can implement mandatory access control (MAC) or discretionary access control (DAC). RBAC is sometimes referred to as role-based security.
- **Least Privilege Principle** – Access privileges for any user should be limited to resources absolutely essential for completion of assigned duties or functions, and nothing more.

Roles and Responsibilities

- **The System Administrator** of each unit is responsible for the technical configuration and monitoring of the access control of each individual based on the roles and access privileges defined by the unit head.
- **The Unit Head** is responsible for deciding the general role and access level of each individual person.
- **The IT Council** will review the Program at least annually to ensure its continued effectiveness.
- **Research Computing Services (RCS)** will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources. RCS is responsible for oversight of each unit in A&GS to ensure IT policy compliance, and provide guidance and education.

Risk Assessment Policy

- A risk assessment shall be performed to identify threats and vulnerabilities involved in the access management process. The associated risk shall be identified and risk levels shall be defined, and appropriate measures shall be taken to address the critical risks in accordance with the A&GS IT Risk Management Program.
- The risk assessment shall be evaluated regularly by each unit to ensure the risks involved are identified with the changing environment, and corrective or improvement actions are appropriate for mitigating the risks. The Policy shall be approved by the ADC and made accessible to every individual in A&GS.

Authorization -Access Granting and Revoking

- Permission is granted only to authenticated users through technology or process controls.

- A&GS utilizes Role-based Access Control (RBAC). Permission and access privileges are determined by the role of the user in A&GS. The unit head defines the access privilege to the resources for the roles in the unit, and system administrators ensure the permission levels are coincident with the roles of the users.
- The principle of least privilege shall be followed when users are granted access. Should changes occurs like job changes, promotion, demotion, transfers, resignation, retirement, disciplinary action, dismissals, etc. the unit head shall inform the system administrator immediately, and appropriate actions shall be taken to change the account accordingly.
- New users must obtain written approval from the unit head to access any information systems in.
- Users can request a change in access via email or written approval from the unit head.
- Should third parties need access into the system, access shall be granted only with the unit head's written approval, and limited to the necessary information. The access must be in accordance with the A&GS Data Classification System.
- The unit head and system administrator shall perform periodic review of user privileges to ensure access is commensurate with user's current responsibilities, and shall pay particular attention toward those accounts of change, removal or inactivation.
- The system administrator shall regularly monitor and track the logging and accessing activities of all accounts, detect unauthorized access, and preserve evidence for those cases of breach.

Authentication

- Authentication is the process of verifying that a user is who they claim to be. Both a public key and private key are involved in the authentication process. An example of a public key is a user name, and that of a private key is a password.
- There are four categories of authentication for desktops and servers within A&GS.
    1. Centralized authentication via OU Active Directory (OU IT)
    2. Authentication via A&GS LDAP or Local AD
    3. Local Desktop Authentication
    4. Local Server Authentication
- Centralized Authentication via OU Active Directory is maintained and controlled by OU IT in accordance with OU Password Policies.
- For local desktop and server authentication (refers to any users who are authenticating locally, without using their 4x4) A&GS relies on standard password requirements for Windows and MAC.
- Local desktops and servers must utilize passwords with a minimum password length of 8-12 characters AND include lowercase and uppercase letters OR numbers and symbols.
- Passwords should expire every 6 months or more often. If expiration cannot be automated, each system administrator should monitor and reset those on a regular basis.
- If necessary, each system administrator can establish stricter password rules covering complexity, minimum length, expiration duration, maximum times of unsuccessful logon, etc.
- Passwords shall be stored with encryption; plain text or easily convertible form must not be used.
- Vender supplied or blank passwords must be reset immediately after installation.

Audit Log Management

The purpose of audit log management is to set up accountability of information systems by providing a trace of user actions, trouble shooting, detecting unauthorized access and intrusion and optimizing systems and networks. A log is a record of the events occurring within an organization's system and networks. Logs are composed of log entries, which contain information related to specific events within a system or network.

- Server logs shall include sufficient information for accountability and traceability, which should include user ID, server startup and shutdown, service startup and shutdown, user account permission modification, IP address or hostname associated with a given event, at the least.
- Server log data is stored on offline archival media, for a minimum of 3 month, and the storage media, in either electronic format or paper copies, is protected from breach of confidentiality, integrity and availability. Only authorized have access to logs, including that unit's system administrators and unit head.
- The system administrator of each unit shall conduct regular analysis on the logs collected, manually or by automated tools.

Privacy and Record Management Program

Purpose

The purpose of this policy is to describe the general principles of A&GS privacy and record management, and raise awareness of relevant laws and regulations.

Definition

- **Confidential Data**: information protected by laws, regulations, policies or contracts, or defined by A&GS and the University of Oklahoma. Some examples include: health care information, social security numbers, student education records, credit card account information
- **Record:** Information that has been recorded on a storage medium and can be retrieved. A record may be a paper, electronic or microfilm document, or video, etc.
- **Confidential Record**: record that contains confidential student, staff or faculty data that should have limited access and be protected from unauthorized disclosure.

Roles and Responsibilities

Each unit shall designate one staff person to be responsible for the record management program. The staff person shall be well trained and understand the general requirements of record management.

Policy

Training of Laws and Regulations

A&GS is subject to a range of federal, state and University of Oklahoma rules and regulations regarding record management. The records with confidential data or sensitive data are particularly protected by these rules. The legislative frameworks include, but are not limited to:

- **FERPA (Family Education Rights & Privacy Act)**

  FERPA is A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

- **GLBA (Gramm-Leach-Bliley Act)**

  GLBA is about the Privacy of Consumer Financial Information, which governs the treatment of nonpublic personal information about consumers by financial institutions

- **HIPAA (Health Insurance Portability and Accountability Act)**

  The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare info and help the healthcare industry control costs.

  Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

  HIPAA protects an individual's health information and his/her demographic information. This is called "protected health information" or "PHI". Information meets the definition of PHI if, even without the patient's name, if you look at certain information and you can tell who the person is then it is PHI. The PHI can relate to past, present or future physical or mental health of the individual. PHI describes a disease, diagnosis, procedure, prognosis, or condition of the individual and can exist in any medium – files, voice mail, email, fax, or verbal communications.

- General Records Disposition Schedules for State Universities and Colleges; Relevant privacy and record management policies of OU; Other related federal and state rules and regulations

Research Computing Services (RCS) will ensure that all personnel in A&GS are provided with the A&GS IT Policies and all supporting documentation and resources. RCS is responsible for oversight of each unit in A&GS to ensure IT policy compliance, and provide guidance and education.

Retention and Maintenance of Records

- Compliance With Laws

  Each unit is advised to maintain records in a consistent and logical manner, to ensure they are in compliance with legal requirements for records protection, storage and disposal.

- Safeguarding and Access Management
  - Safeguarding measures shall be taken to protect the records with confidential information from unauthorized access, exposure, usage and disposal.
  - Confidential records shall be stored and kept in a restricted area with safeguarding protection. Only authorized personnel can have access to these records.
  - The communication and distribution of these records shall be under strict control.
  - For computers with confidential data, access control and secure passwords shall be utilized and only authorized users will have access.

- Backup

  For important or critical electronic records, backups are conducted regularly by the system administrator; the backup tapes and media are stored in appropriate onsite and offsite locations with appropriate environmental conditions in accordance with the Business Continuity and Disaster Recovery Program.

- Disposal of Records

  If the decision is made to destroy or dispose of records, this must be done in compliance with applicable laws. Shred paper records with confidential data, and erase or destroy electronically stored records, with the assistance of the system administrator for your unit.

- Regular Evaluation

  Each unit shall perform annual evaluation on the effectiveness of the current safeguarding method and take improvement actions when necessary.

Appendix

Business Continuity and Disaster Recovery Program - BIA

Business Impact Analysis Form

Restoration Priority	Resource/Service/ Function	Owner	Service Outage Impact (H/M/L)	Recovery Time Objective (RTO)	Resources/process required for resource restore/resume
	Basic infrastructure				
1	Power	FM	H	24 hr	UPS and generator backup
1	HVAC	FM	H	24 hr	UPS and generator backup
0.5	Space	A&GS	H	1 week	alternate site available
1	Communication	OU IT	H	24 hr	
	IT related services				
1	Software	unit	H	24 hr/next bus day	
1	Hardware	unit	H	24 hr/next bus day	
0.1	Printing/scanning function	unit	L	1 week	
0.9	A/V equipment	unit/ RCS	H	24 hr	
0	Camera / Web camera	unit	L	n/a	
0.9	Remote Access services	unit	H	24 hr	
	Networking service				
1	Router	OU IT	H	24 hr	
1	Switch	OU IT	H	25 hr	
1	DNS service	OU IT	H	26 hr	
1	firewall	OU IT	H	27 hr	
	Internet Connectivity				
0.5	Main site	Web-comm	M	48 hr	
0.1	Recovery Site	RCS	L	48 hr	
	Data backup				
1	Loss of high priority data	unit	H	24 hr	
0	Loss of low priority data	unit	L	n/a	
1	Loss of primary site	RCS	H	24 hr	

Risk Assessment

Risk Rating Matrix

Risk Likelihood	Risk Impact		
	High	Moderate	Low
High	High	Moderate	Moderate
Moderate	Moderate	Moderate	Low
Low	Moderate	Low	Low

Risk Assessment Form

Risk Statement	Likeli-hood (LMH)	Impact (LMH)	Risk Rating (LMH)	Mitigation & Contingency Recommendations
Application software flaws could compromise confidentiality and integrity of data	L	H	L	Review and implement patches and upgrades (vendor supplied or reputable source only) in a timely manner
OS software flaws could compromise confidentiality and integrity of data	L	H	L	Review and implement patches and upgrades (vendor supplied or reputable source only) in a timely manner
Remote access currently if not in place could result in compromise of confidentiality and integrity of data	M	H	M	A&GS IT systems admins will follow appropriate guidelines in Access Management Policy
Loss or theft of data from server could result in compromise of confidentiality and integrity of corporate data	L	H	L	A&GS IT systems admins will follow appropriate guidelines in Access Management Policy
Hardware Issues/Equipment Failure or loss	L	H	L	Backups performed regularly and copied off-site to alternate site location

Poor Systems Administration Practices External to Information systems and Database Administration	L	H	L	Review and implement patches and upgrades (vendor supplied or reputable source only) in a timely manner
Key Person Dependency	M	H	M	Cross-training when possible; passwords and access procedures shared with another IT system administrator
Loss of Critical Documentation, Data or Software	L	H	L	Set up secure location for file sharing of documentation
Clear Text Transmission of Critical Data	L	H	L	Utilize secure methods of transmission only
Data Disclosure	M	H	M	A&GS IT systems admins will follow appropriate guidelines in Access Management Policy
Software Issues from Vendor	M	H	M	Keep maintenance agreements up-to-date; insure no unsupported releases in use
Poor Password Practices	L	H	L	A&GS IT systems admins will follow password guidelines in Access Management Policy
System Compromise	L	H	L	Maintain all system components at appropriate release levels and closely monitor system for unauthorized access.
Lack of Sufficient Operational Policies	L	M	L	New A&GS Policies created and will be provided to all A&GS personnel
Poor Physical Security	L	H	L	All data centers are secured with key card access. May install cameras for monitoring
Environmental Issues	L	H	L	Maintain equipment at optimum efficiency, replace equipment on the manufacturer's recommended cycle, and maintain contracts for equipment maintenance
Natural Disaster	L	H	L	Maintain and test disaster recovery plans

Business Continuity and Disaster Recovery Program Contact Lists

A&GS IT Council Contact List

Bostic, Jared	jpbostic@ou.edu	OCS
Cook, Chris	cscook@ou.edu	CAPS
Glass, Jason	jglass@ou.edu	RCS
Greenwood, Bill	wgreenwood@ou.edu	CSA
Ho, Desmond	desmond@ou.edu	OWS
Holcomb, Ben	bholcomb@ou.edu	SOM
Keys, Alicia S.	akeys@ou.edu	RCS
McCord, Matt	mmccord@ou.edu	ARRC
Riley, Shawn	rileysp@ou.edu	SOM
Skaggs, Gary	gskaggs@ou.edu	OU IT NOC

A&GS Director's Council Contact List

Duca-Snowden, Victoria	vduca@ou.edu	NASA SG
Earsom, Eugene	earsom@ou.edu	OKAGE
Fiebrich, Chris A.	fiebrich@ou.edu	OCS Mesonet
Goodman, Nathan	goodman@ou.edu	ARRC
Guthrie, Tanya	tguthrie@ou.edu	DEAN
Hempe, Mary Anne	mahempe@ou.edu	DEAN
Keys, Alicia S.	akeys@ou.edu	RCS
Kloesel, Kevin	longhorn@ou.edu	OCS
Maxon, Chris A.	cmaxon@ou.edu	DEAN
McPherson, Renee A.	renee@ou.edu	SCCSC
Moore, Berrien	berrien@ou.edu	DEAN
Parsons, David	dparsons@ou.edu	SOM
Peppler, Randy A.	rpeppler@ou.edu	CIMMS
Puls, Robert W.	bpuls@ou.edu	OWS
Scott, Melissa L.	mscott@ou.edu	CSA
Tarhule, Aondover	atarhule@ou.edu	DGES
Xue, Ming	mxue@ou.edu	CAPS
Yu, Tian-You	tyu@ou.edu	ARRC

A&GS College Personnel Contact List

Barnhill, Debbie	dbarnhill@ou.edu	SOM	325-6561
Bowers, Heather	hbowers@ou.edu	Security	618-3666
Campbell, Nancy	ncampbell@ou.edu	SOM	
Guthrie, Tanya	tguthrie@ou.edu	DEAN	325-3037
Hempe, Mary Anne	mahempe@ou.edu	DEAN	325-9035
Leffler, Greg	gleffler@ou.edu	NWC Dock	325-1850
Marsh, Deborah	dmarsh@ou.edu	DGES	325-5325
Murphy, Heather	hmurphy@ou.edu	DEAN	325-3061
Sallee, Lee Anne	lasallee@ou.edu	DEAN	325-3095
Sexton, Dale	dsexton@ou.edu	DEAN/FM	590-6750
Steely, Becky	bsteely@ou.edu	SOM	325-6561
Upchurch, Christie	cupchurch@ou.edu	SOM	325-6561

Add unit Admins – see A&GS Contact List

External and Vendor Contact List

OU FM (power, UPS, HVAC)	email@ou.edu	325-3060
OU IT (network, telecom)	needhelp.ou.edu	325-4357 (Helpdesk)
OU IT Store (hardware/software)	itstore@ou.edu	325-1925
OU Printing Services (printer lease)	printing@ou.edu	325-4176
RK Black (printer services)		321-5900
Best Buy (hardware/software)		573-9613