



# Information Security Policies

Notice: Information contained in this document is classified as Agusan del Sur State College of Agriculture and Technology (ASSCAT) Confidential Proprietary. No person outside ASSCAT shall have access to the information contained in this document unless the College approves it. Otherwise, it is the responsibility of the person knowing the information contained in this document to ensure its confidentiality of it and to prevent unauthorized access to it.

Uncontrolled copy if printed/photocopied (unless specified otherwise)



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## TABLE OF CONTENTS

A.	Introduction .....	3
B.	Definition of Terms .....	4
C.	Policies .....	6
I.	Acceptable Encryption Policy .....	6
II.	Acceptable Use Policy .....	8
III.	Access Rights and Control Policy .....	13
IV.	Acquisition And Merger Assessment Policy .....	18
V.	Backup Policy .....	21
VI.	Classification of Information Policy .....	23
VII.	Cloud Services Policy .....	25
VIII.	Computer Laboratory Security Policy .....	27
IX.	Data Center Security Policy .....	31
X.	Database Credentials Coding Policy .....	35
XI.	Disaster Recovery Plan Policy .....	38
XII.	Email Policy .....	40
XIII.	Endpoint Devices Policy .....	44
XIV.	Information Transfer Policy .....	48
XV.	Intellectual Property Rights .....	50
XVI.	Labelling of Information Policy .....	51
XVII.	Password And Authentication Policy .....	54
XVIII.	Project Management Policy .....	57
XIX.	Remote Access Policy .....	59
XX.	Software Installation Policy .....	61
XXI.	Storage Media Policy .....	63
XXII.	Supplier Relationship Policy .....	65
XXIII.	System Change Management Policy .....	67
XXIV.	System Deployment and Test Policy .....	70
XXV.	System Development Policy .....	72
XXVI.	Technology Equipment Disposal Policy .....	75
XXVII.	Web Application Security Policy .....	77
XXVIII.	Wireless Communication Policy .....	80
XXIX.	Wireless Communication Standard .....	84
D.	Compliance and Monitoring .....	86
E.	Revision History .....	87



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## A. INTRODUCTION

Information is a critical asset in this institution, the Agusan del Sur State College of Agriculture and Technology (ASSCAT), and safeguarding it is essential in maintaining its competitive edge, reputation, and operational integrity. This Information Security Policy aims to establish a framework for protecting ASSCAT's information assets from unauthorized access, disclosure, alteration, and destruction. This policy outlines the responsibilities, principles, and practices that all members of this institution must adhere to ensure its information resources' confidentiality, integrity, and availability.

This policy is intended to guide ASSCAT's employees, contractors, and stakeholders in understanding and implementing effective information security measures. It provides a comprehensive set of guidelines and procedures that encompass the management of information security risks, the proper handling of sensitive information, and the use of technology securely.

This Information Security Policy is designed to comply with relevant legal, regulatory, and contractual requirements, and it reflects the institution's best practices. By following this policy, we aim to create a secure environment that supports ASSCAT's objectives and fosters trust among our clients, partners, and employees.

The Information Security Policy, along with its supporting controls, processes, and procedures, applies to all information utilized at ASSCAT in any format. This includes information processed by other organizations in their dealings with ASSCAT.

Furthermore, the Information Security Policy and its supporting mechanisms apply to all individuals with access to ASSCAT's information and technologies, including external parties that provide information processing services to the institution.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## B. DEFINITION OF TERMS

**Access Control** - The process of granting or restricting access to information assets based on predefined policies and rules.

**Advanced Encryption Standard (AES)** - An encryption standard being developed by NIST to specify an unclassified, publicly disclosed, symmetric encryption algorithm.

**Critical Data** - Data that is essential for the operation of the college and whose loss would cause significant disruption to operations and services.

**Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)** is an IETF open standard that's defined in RFC 5216. More colloquially, EAP-TLS is the authentication protocol most commonly deployed on WPA2-Enterprise networks to enable the use of X. 509 digital certificates for authentication.

**Flexible Authentication via Secure Tunneling (EAP-FAST)** - authenticates using a PAC (Protected Access Credential) which can be managed dynamically by the authentication server.

**Firewall** - A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

**Hash Function** - (cryptographic) hash functions are used to generate a one-way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

**Honeypot** - Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

**LDAP** - A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or an institutional Intranet.

**Least Privilege** - The principle of providing users with only the minimum level of access rights or permissions required to perform their job functions.

**MAC Address** - A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

**Need-to-Know** - the principle of providing users with access to information assets only if necessary for their duties or responsibilities.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

**Protected Extensible Authentication Protocol**, also known as Protected EAP or simply PEAP, is a protocol that encapsulates the Extensible Authentication Protocol within an encrypted and authenticated Transport Layer Security tunnel.

**Proprietary Information** - is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

**Ransomware** - A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

**Spam** - Electronic junk mail or junk newsgroup postings.

**Service Set Identifier (SSID)** - A unique ID that can be made up of case-sensitive letters, numbers, and special characters like dashes, periods, and spaces. According to the 802.11 wireless local area networks (WLAN) standard, an SSID can be as long as 32 characters.

**Temporal Key Integrity Protocol (TKIP)** is an encryption protocol included in the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard for wireless local area networks (WLANs).

**Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)** - is a system of encryption used to authenticate users on wireless local area networks.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## C. POLICIES

### I. ACCEPTABLE ENCRYPTION POLICY

#### Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that national regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the Philippines.

#### Scope

This policy applies to all employees and affiliates.

#### Policy

#### Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the [IETF/IRTF Cipher Catalog](#), or the set defined for use in the National Privacy Commission Circular 16-1, Rule II, Section 8, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

#### Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Consider <a href="#">RFC6090</a> to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. <a href="#">PKCS#7 padding scheme</a> is recommended. Message hashing is required.
LDWM	SHA256	Refer to <a href="#">LDWM Hash-based Signatures Draft</a>



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Hash Function

### Key Agreement and Authentication

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- Endpoints must be authenticated before the exchange or derivation of session keys.
- Public keys used to establish trust must be authenticated before use. Examples of authentication include transmission via cryptographically signed messages or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

### Key Generation

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see [NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2](#).

### Related Standards, Policies, and Processes

National Privacy Commission Circular 16-1, Rule II, Section 8,

- Proprietary Encryption



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## II. ACCEPTABLE USE POLICY

### Overview

The Information Security Committee intends to publish an Acceptable Use Policy that aligns with the institution's established culture of openness, trust, and integrity. This policy is not meant to impose unnecessary restrictions, but to protect its employees, partners, and the institution from illegal or harmful actions, whether intentional or unintentional.

All Internet-/Intranet-/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, and network accounts (e.g., email, web browsing, FTP), are the property of the institution. These systems are for business purposes, supporting the needs of the institution and our clients and customers during normal operations.

Effective security requires the participation and support of every employee and affiliate who interacts with information and information systems. It is the responsibility of all computer users to understand and follow these guidelines in their daily activities.

### Purpose

This policy outlines the acceptable use of computer equipment and other electronic devices in the institution, aiming to protect both employees and the institution. Inappropriate use can expose to various cyber risks, including virus attacks like ransomware, compromised network systems and services, data breaches, and legal consequences.

### Scope

This policy covers the use of information, electronic and computing devices, and network resources during any activity related to the institution's business or interaction with internal networks and systems, regardless of ownership (whether belonging to Institution, the employee, or a third party). This includes all employees, contractors, consultants, temporary workers, and other personnel associated with the Institution and its subsidiaries. Everyone covered by this policy is responsible for exercising good judgment and adhering to Institution's policies, standards, and local laws and regulations concerning the appropriate use of information, electronic devices, and network resources.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Policy

### General Use and Ownership

#### Ownership and Protection of Information

- All Institution proprietary information stored on electronic and computing devices, regardless of ownership (Institution, employee, or third party), remains the sole property of the Institution.
- Promptly report any theft, loss, or unauthorized disclosure of Institution proprietary information.
- Access, use, and share Institution proprietary information only to the extent authorized and necessary to fulfill your assigned job duties

#### Personal Use

- Exercise good judgment regarding the reasonableness of personal use of Internet/Intranet/Extranet systems.
- Individual units are responsible for creating guidelines for personal use. Refer to unit policies, and consult unit heads, Vice Presidents or Digital Transformation Center if uncertain.

#### Monitoring and Auditing

- Authorized individuals within Institution may monitor equipment, systems, and network traffic at any time for security and network maintenance purposes, including during Infosec audits.
- Institution reserves the right to periodically audit networks and systems to ensure compliance with this policy.
- In the event of litigation, users are required to cooperate with the institution by providing access to their mobile devices as needed.

#### Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Access Control Policy.
- System-level and user-level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from institutional email addresses to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Institution unless posting is during business duties.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

## Unacceptable Use

- The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).
- Under no circumstances is an employee of Institution authorized to engage in any activity that is illegal under local, regional, national, or international law while utilizing Institution-owned resources.
- The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

## System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or institution protected by copyright, trade secret, patent, or other intellectual property, or other applicable laws, including but not limited to the installation or distribution of pirated or other software products that are not appropriately licensed for use by the Institution.
- Unauthorized copying of copyrighted material, including but not limited to digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Institution or the end user does not have an active license.
- Accessing data, a server or an account for any purpose other than conducting the Institution's business is prohibited, even if you have authorized access.
- Exporting software, technical information, encryption software, or technology in violation of international, and national export control laws is illegal. The appropriate management should be consulted before the export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, ransomware, etc.).
- Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the Institution's computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any of the Institution's accounts.
- Making statements about warranty, expressly or implied, unless it is part of normal job duties.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to, accessing data of which the employee is not an intended recipient. They also include logging into a server or account that the employee is not expressly authorized to access unless these duties are part of regular job duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Information Security Committee is made.
- Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is part of the employee's normal job duties.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the Institution's network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Institution's employees to parties outside Institution.

## Email and Communication Activities

- When using institutional resources to access and use the Internet, users must understand they represent the institution. Whenever employees state an affiliation to the institution, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the institution."
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Institution's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Institution or connected via Institution's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Blogging and Social Media

- Occasional and limited use of the Institution's social media accounts to engage in blogging or other online posting is acceptable, provided that it is conducted professionally and responsibly, does not violate Institution's policies, does not harm Institution's interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from Institution's systems is also subject to monitoring.
- Therefore, Employees are prohibited from disclosing any Institution's confidential or proprietary information, trade secrets, or any other material covered by the Institution's Confidential Information policy when engaged in blogging.
- Employees must avoid making discriminatory, disparaging, defamatory, or harassing. They shall not engage in any blogging that may damage or harm the image, reputation, or goodwill of the Institution or any of its employees.
- When expressing personal statements, opinions, or beliefs in their blogs, employees must not imply or state they are acting as an employee or representative of the Institution. Employees assume any risk associated with blogging.
- In addition to complying with all laws regarding copyrighted or export-controlled materials, the Institution's trademarks, logos, and any other Institution's intellectual property may not be used in connection with any blogging or social media activity.

## Related Standards, Policies, and Processes

- Data Classification Policy
- Data Protection Standard
- Access Policy
- Password Policy



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## III. ACCESS RIGHTS AND CONTROL POLICY

### Overview

The institution implements physical and logical access controls across its networks, IT systems, and services to provide authorized, granular, auditable, and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity, and availability by the Information Security Policy.

Access control systems are in place to protect the interests of all authorized users of the institutional IT systems, as well as data provided by third parties, by creating a safe, secure, and accessible environment in which to work.

### Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements.

### Scope

This includes the physical and logical access rights of information assets.

### Policy

#### Roles and Responsibilities

**Data Owners** - Data Owners are responsible for defining the access control requirements for the information they own or manage. They should classify data according to its sensitivity and specify the appropriate access control based on the Classification of Information and Labelling of Information Policy.

**System Administrators** - System Administrators are responsible for implementing and maintaining access controls on the information systems and resources under their jurisdiction. They must ensure that access controls are aligned with the data owner's requirements and based on the Classification of Information and Labelling of Information Policy. They shall also be responsible for overseeing the implementation and enforcement of this Access Control Policy.

**Users/Employees** - All users are responsible for complying with the access control policies and procedures defined by the institution. They must use their assigned credentials only for authorized purposes, protect their access credentials from unauthorized disclosure, and report any access control violations or concerns to the appropriate authorities.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## General Guidelines

- Access to information shall be granted based on the principles of least privilege and need-to-know.
- Access rights shall be granted, modified, or revoked based on defined roles, responsibilities, and job functions.
- Access controls shall be implemented and enforced across all information systems and facilities to prevent unauthorized access, modification, disclosure, or destruction of information assets.
- An individual is only assigned access to information technology infrastructure when a clear need is present.
- All physical facilities with restricted areas must be monitored and secured with physical security mechanisms. Only allowed personnel identified by the Owner: are allowed to access the restricted areas, facilities, and equipment.
- Digitized information has assigned levels of access rights set by the owner. Only connected and active employees or students associated with specific documents have access to those documents.
- Hard copies of documents shall be maintained in separate folders or facilities, which are accessible only to individuals authorized to work with each kind of data.
- Portable information, such as data stored in flash drives, must be physically secured and must not be left unattended. For instance, do not leave it in a parked car or coffee shop; wherever possible, hold and guard laptops and information storage devices personally.
- The person responsible for information classified as “Confidential” or “Restricted” shall position the screen so that it is difficult for others to see when viewing on a computer. The information must be promptly removed from view after use.
- Do not leave printed materials and copies lying around. Collect copies from copiers and scanners immediately.
- User access shall be managed through a formal access control process, including user registration, authentication, authorization, and auditing.
- All access control mechanisms shall be regularly reviewed, tested, and updated to ensure their effectiveness and compliance with security requirements.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Any deviations or exceptions to this policy must be authorized by the top management and documented.
- Violations of this policy may result in disciplinary action, termination of employment, legal action, or other consequences as deemed appropriate by the organization.

## Access Control Measures

### User Identification and Authentication

#### Account Creation

- User accounts will be created for all authorized users based on their roles and responsibilities.
- Institutional accounts and access to information systems are automatically created upon enrollment for students and employment for employees.
- Accounts will be provisioned and managed by the Digital Transformation Center through a secure and documented process.
- The creation of Privileged accounts and/or Special Accounts for information systems shall be designated and identified by the Owner. Access to privileged accounts will only be granted when deemed necessary and authorized by the Owner.
- Enroll in 2-factor authentication for institutional accounts.

#### Special Accounts and Access Revocation:

- Privileged accounts for information systems are identified by the Owner. No privileged accounts will be granted unless necessary and approved by the Owner.
- Access rights will be disabled or removed when the IT Team receives a notification that a user has revoked access to institutional systems.

#### Password Management

- Users must choose strong, unique passwords that meet the following requirements:
- Minimum length of 12 characters.
- Combination of upper- and lower-case letters, numbers, and special characters.
- Changed at least every 365 days.
- Passwords must not be shared or stored in an unsecured manner.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 16 of 87

**Authentication:**

- Multi-factor authentication (MFA) will be implemented for accessing systems unless an exception has been granted by the Director of the Digital Transformation Center.
- MFA methods may include tokens, smart cards, biometrics, or other approved mechanisms.
- Institutional accounts shall be enrolled in 2-factor authentication.

**Identity Verification:**

- Verification of the user's identity must be performed by Information System Customer Support before granting a new password.
- For students: An e-copy of Certificate of Registration or Student ID.
- For Employees: An e-copy of Employee ID.

**Access Control Policies:****Least Privilege:**

- Access privileges will be granted based on the principle of least privilege, meaning users will be granted only the access necessary to perform their job functions.
- Access to 'Confidential' and 'Restricted' information will be limited to authorized persons whose job or study responsibilities require it, as determined by law, contractual agreement with interested parties, or the Information Security Policy.
- Requests for additional access privileges must be approved by the data owner and documented.

**Physical Access Control**

- Physical access to facilities, data centers, server rooms, and other sensitive areas shall be restricted to authorized personnel only.
- Access control measures such as access badges, biometric scanners, surveillance cameras, and security guards shall be implemented to prevent unauthorized entry or tampering.

**User Access Review:**

- Existing user accounts and access rights will be reviewed at least annually to detect:
  - Inactive accounts
  - Accounts with unnecessary privileges, such as:
  - Active accounts assigned to third parties, suppliers, or employees no longer connected to the institution.
  - System administrative rights granted to non-administrators.
  - Accounts of users who have changed roles or jobs.
  - Unknown active accounts.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Access Termination:

- When a user's employment or affiliation with the institution is terminated, their access privileges will be promptly revoked.
- Access rights will be disabled or removed when the IT Team receives a notification that a user has revoked access to institutional systems.
- Access termination procedures will be documented and followed to ensure that all accounts and credentials associated with the user are deactivated.

## Logging and Monitoring

- Access control mechanisms will be implemented to record and monitor user activities within the information systems.
- System logs and audit trails will be regularly reviewed for unauthorized access attempts or suspicious activities.
- An incident response plan will be in place to address security incidents or breaches related to access controls.
- Regular security assessments and audits shall be conducted to evaluate the effectiveness of access controls and identify vulnerabilities or weaknesses.

## Third-Party Connection Agreement

- All new connections between third parties and the institution are required to agree to a Non-disclosure Agreement ("NDA") before obtaining approval to access information, systems, and other documents. This agreement must be signed by the authorized executive of the sponsoring office as well as a representative from a third party who is legally empowered to sign on behalf of the third party.
- The DTC team shall maintain a current list of external contractors or suppliers having access to institutional systems.
- Termination of access will start on the date of termination of the contract. Unless there are technical supports and maintenance included in the contract.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## IV. ACQUISITION AND MERGER ASSESSMENT POLICY

### Purpose

The purpose of this policy is to establish our organization's responsibilities regarding institutional acquisitions and mergers. This policy also defines the minimum-security requirements involved in the Information Security acquisition assessment.

### Scope

This policy applies to all campuses under the institution and pertains to all systems, networks, laboratories, test equipment, hardware, software, and firmware, owned and/or operated.

The process of integrating a newly acquired campus can have a drastic impact on the security posture of either the main campus or the satellite campuses. Both entities' network and security infrastructure may vary greatly, and the new campus's workforce may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

- Assess the institution's security landscape, posture, and policies.
- Assess resources for integration and security, including budgeting for upgrades, tools, training, and hires if needed.
- Protect both main and the satellite campuses from increased security risks.
- Educate acquired or newly established campus team members about institutional policies and standards.
- Adopt and implement institutional Security Policies
- Integrate satellite campuses
- Continuous monitoring and auditing of the satellite campuses.

### Policy Statements

#### General

Acquisition assessments are conducted to ensure that a campus under the institution does not pose a security risk to institutional networks, internal systems, and/or confidential/sensitive information. The Information Security Committee will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Information Security role is to detect and evaluate information security risks, develop a remediation plan with the affected parties for the identified risk, and work along with the acquisitions team to implement solutions for any identified security risks, before allowing connectivity to institution's networks. Below are the minimum requirements that the acquired campus must meet before being connected to the institutional network.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Hosts

- All endpoints (servers, desktops, laptops) will be replaced or re-imaged with the institutional standard security baseline configuration and will be required to maintain this minimum standard.
- Business critical production servers that cannot be replaced or re-imaged must be audited 2 times for internal and 1 external. There must be an exception granted and documented by the Information Security Team.
- All end-point computing devices will require approved anti-virus protection and/or Endpoint Detection and Response software (EDR) before a network connection is established.
- Access to sensitive data and critical systems should be restricted to authorized personnel only
- Hosts must be configured securely based on industry standards and organizational policies.
- Default configurations should be changed, and unnecessary services disabled.
- Hosts must have logging enabled to track security events and anomalies.
- Regular monitoring of logs should be conducted for suspicious activities.
- Regular backups of host data must be performed and stored securely.
- Procedures for quick recovery in case of data loss or system compromise should be established.
- Users and administrators of hosts must receive regular security training.
- Awareness campaigns should highlight the importance of host security and best practices.

## Networks

- All network devices will be replaced or re-imaged with the institutional standard baseline configuration.
- Wireless network access points will be configured to the institutional standard baseline configuration.
- The acquired institution's network must comply with institutional network standard security baseline configuration.
- Networks must be logically segmented to isolate sensitive data and critical systems.
- Firewalls must be deployed at network perimeters to control incoming and outgoing traffic.
- IDPS should be implemented to detect and prevent suspicious network activities.
- Regular updates and tuning of IDPS rules are essential for effectiveness.
- Wireless networks must use strong encryption (e.g., WPA3) and secure authentication methods.
- SSID broadcasting should be disabled, and default settings changed.
- Regular vulnerability scans of the network infrastructure must be conducted.
- Identified vulnerabilities should be promptly patched or mitigated.
- Network devices must have logging enabled to track security events and activities.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Centralized log management and regular review of logs are required. Network devices (routers, switches, etc.) should be hardened with secure configurations.
- Default credentials must be changed, and unnecessary services disabled.
- Detailed documentation of the network topology, configurations, and security measures should be maintained.
- This documentation is essential for audits, troubleshooting, and incident response.

## Internet

- All Internet connections will be terminated.
- When justified by business requirements, air-gapped Internet connections will require the Information Security Committee's review and approval.

## Remote Access

- All remote access connections will be terminated.
- Remote access to any production, test, development, or guest network will be provided by the institution.

## Labs

- Lab equipment must be physically separated and secured from non-lab areas.
- The lab network must be separated from the institution's production network with a Virtual network (VLAN) with a firewall between the two networks.
- Any direct network connections to external customers, partners, etc., must be reviewed and approved by the Information Security Committee or the Lab Technicians.
- Implement application whitelisting to allow only approved applications to run on laboratory systems.
- Unauthorized software installations should be prevented.
- Enable logging on laboratory systems to track security events and activities.
- Regularly monitor logs for unusual or suspicious behavior.
- All acquired lab networks must conform with the LabTech standard security baseline configuration.
- In the event the acquired networks and computer systems fail to meet these requirements, the institution's Chief Information Security Officer (CISO) must acknowledge and approve of the risk to institutional networks.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## V. BACKUP POLICY

### Overview

The electronic data of institution needs to regularly copy its electronic information to secure storage (backups) in case of emergencies or disruptions. This policy sets the minimum standards for creating and keeping these backups. Special cases requiring more frequent or extensive backups will be handled individually.

### Purpose

Ensure the essential data is consistently backed up to protect against accidental and intentional data loss, corruption, disasters, or other unforeseen incidents. To establish and maintain the *practice* of protecting data through regular backups.

### Scope

The DTC staff and *Departments in the institution* are responsible for managing electronic data. It covers data stored on servers, and virtual machines, as well as data hosted with cloud service providers. This ensures institutional work can quickly continue with minimal data loss.

### Policy Statement

The institution commits to maintaining *robust* data backup and recovery processes to safeguard the integrity and availability of data in the event of hardware failure, software failure, human error, or natural disasters.

### Virtual Machines and Databases

- Perform a minimum of three backup schedules daily
- Maintain at least ten (10) recovery points for six months
- Store at least one fully recoverable backup version off-site, which can be in a secure facility separate from the main campus or with a cloud service provider.
- Test backup media quarterly to ensure integrity and recoverability. Do not overwrite or alter the original storage media during testing
- Encrypt all backup data and restrict user access to authorized personnel.  
Data from the cloud service provider must also have backup schedules.

Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## **Institutional Documents**

All institutional documents stored in workstations, laptops, or other portable devices should have an automatic backup in the Google Workspace account using their institutional accounts.

When working outside of the institution's premises, employees must exercise heightened vigilance in safeguarding backup files containing confidential information.

## **Requirements**

### **Physical Security**

Backup media must be stored in secure locations with controlled access, such as locked cabinets, vaults, or secure data centers.

Access to these locations must be restricted to authorized personnel.  
Logs of access and activity should be maintained.

Physical security measures should be in place to protect against unauthorized access, theft, vandalism, and environmental hazards (e.g., fire, and water damage).

### **Environmental Protection**

Backup media must be stored in controlled environments with appropriate temperature, humidity, and other environmental conditions. These conditions should meet or exceed the manufacturer's recommendations for the specific media type.

Environmental monitoring systems should be in place to detect and alert for deviations from acceptable conditions.

Disaster recovery plans should be developed and tested to ensure timely and effective recovery of backup information in the event of a major disaster.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## VI. CLASSIFICATION OF INFORMATION POLICY

### Purpose

To ensure identification and understanding of protection needs of information by its importance to the organization and to protect sensitive data from being shared with unauthorized personnel, published on the internet, and so on.

### Scope

Information Assets are information generated by or for, owned by, or otherwise in the possession of the institution that is related to the college's activities. These assets may exist in any format (i.e., digitized, paper, electronic) and include but are not limited to all academic, administrative, finance, research, and production, as well as the computing infrastructure program code that supports the business of the institution.

### Policy

- In this policy, the Information Assets of the institution shall be classified into 2 categories based on the level of information sensitivity, availability, and the impact of disclosure to the organization. The following information classifications shall be utilized across all levels of the college to ensure protective control is in place.
  1. **Public Information** – refers to data, records, documents, or knowledge that is made available and accessible to the general public without restrictions. This information is often disseminated by government entities, organizations, or individuals for public awareness, transparency, and accountability. Public information can exist in various formats, including digital or physical, and it encompasses a wide range of content across different domains. Disclosure of this kind of information causes no harm to the organization.
  2. **Restricted Information** – refers to data, records, or knowledge that is classified or marked to limit access, distribution, or disclosure due to its sensitive or confidential nature. This type of information is typically subject to controls and regulations governing its access and handling to prevent unauthorized exposure or misuse. Restricted Information is further classified into Internal Information and Confidential Information.
    - **Internal Information** – refers to data, records, or knowledge that is specifically created, collected, used, and maintained within an organization for its operations and purposes. This type of information is not generally intended for public disclosure and dissemination and is often kept confidential or restricted to authorized personnel within the organization. Disclosure of internal information causes minor operational inconvenience.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- **Confidential Information** – refers to sensitive data, records, or knowledge that is legally protected or marked as private and is intended to be kept secret or disclosed only to authorized individuals or entities. This information holds significant value for an organization, and its unauthorized disclosure, access, or use could lead to severe financial, legal, or reputational harm and a serious impact on long-term strategic objectives.

## Policy Statement

- Owners of information shall be accountable for the classification of data under this policy. They are responsible for analyzing and understanding information assets and assigning a level of sensitivity to each.
- Owners of information must assess the level of risk according to the probability that harm will occur and the extent of that harm should the data be lost, stolen, or accessed by unauthorized parties.
- If information is created jointly by more than one department, all involved departments must cooperatively classify the information.
- Owners of information are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of institution data in compliance with this and related policies.
- Any unauthorized disclosure or loss of information assets aside from public information must be reported to the Information Security Response Team.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## VII. CLOUD SERVICES POLICY

### Purpose

To specify and manage information security for the use of cloud services

### Scope

All acquisition, use, management, and exit from cloud services.

### Policy

#### **The Cloud Service Provider Obligations for Data Protection and Service Availability:**

- Providing solutions based on industry-accepted standards for architecture and infrastructure.
- Managing access controls of the cloud service to meet the institution's requirements.
- Implementing malware monitoring and protection solutions.
- Processing and storing the institution's sensitive information in approved locations (e.g., a particular country or region) or within or subject to a particular jurisdiction.
- Providing dedicated incident response support in the event of an information security incident in the cloud service environment.
- Ensuring that the institution's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted).
- Supporting the institution in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions.
- Providing appropriate support and availability of services for an appropriate time frame when the institution wants to exit from the cloud service.
- Providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by the institution.
- Providing and returning information such as configuration files, source code, and data that are owned by the institution upon request.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Acting as the cloud service customer by contractual agreements when requested during the service provision or at the termination of service.

## Secure Usage of Cloud Services

- Requires identification of all users, documentation of cloud service types (SaaS, PaaS, IaaS) with detailed specifications, and data classification with encryption for sensitive information.
- Implement multifactor authentication (MFA) for all users accessing cloud services to enhance security by requiring multiple forms of authentication before granting access.

## Utilization of Cloud Services

- To utilize a cloud service for institutional purposes, submit a written request to the DTC Office.
- The DTC team will collaborate with the requesting department to assess the sensitivity of the institutional data involved.
- The requesting officer shall be required to sign a Non-Disclosure Agreement (NDA) to ensure the highest standards of data security and privacy are upheld
- All users are responsible for adhering to all applicable laws and regulations and IT security policies.

## Security Control Assessment

The DTC team will conduct a comprehensive assessment of security control assessment every six months. The assessment will include reviewing all security settings and investigating failed access attempts to find areas that could be improved.

## Security Incident Recovery

Establish an Incident Response Team as the group responsible for dealing with security issues that involve cloud environments. All members are required to go through regular training to ensure preparedness with the incident response process.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## VIII. COMPUTER LABORATORY SECURITY POLICY

### Overview

The Computer Laboratory Security Policy of the institution aims to protect computer resources by implementing access control measures, data encryption, network security protocols, software management guidelines, incident response procedures, and ongoing training initiatives.

### Purpose

This policy establishes the information security requirements to help manage and safeguard laboratory resources and institutional networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

### Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at ASSCAT and its campuses must adhere to this policy. This policy applies to institution-owned and managed laboratories.

### Policy

#### General Requirements

- The Computer Laboratory In-Charge is responsible for assigning Computer Lab Technicians, a point of contact (POC), and a backup POC for each lab. The Computer Lab In-Charge must maintain up-to-date POC information with the ICT Director. Lab managers or their backup must be available around the clock for emergencies, otherwise, actions will be taken without their involvement.
- Computer Lab Technicians are responsible for the security of their labs and the lab's impact on the institutional production network and any other networks. Computer Lab Technicians are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined Computer Lab In-Charge must do their best to safeguard ASSCAT from security vulnerabilities.
- Computer Lab Technicians are responsible for the lab's compliance with all ASSCAT security policies. As well as to be present on the approved schedule utilization of the computer laboratories. That includes overseeing the students' computer utilization during laboratory sessions/scheduled.
- The Computer Lab Technicians are responsible for controlling lab access. Access to any given lab will only be granted by the Computer Lab In-Charge or the ICT Director and other higher authorities. This includes continually monitoring the



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

access list quarterly to ensure that those who no longer require access to the lab have their access terminated. As well as monitoring the physical equipment inside the computer lab ensuring that all equipment is placed and complete.

- All user passwords must comply with ASSCAT's Password Policy.
- Individual user accounts on any lab computers must be logged out after utilizing. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months).
- PC-based lab computers must have the institution's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed/isolated from the network until they are verified as virus-free. Computer Lab Technicians are responsible for ensuring the anti-virus software runs and its antivirus definitions are up-to-date at regular intervals, and that computers are verified as virus-free.
- Any activities to create and/or distribute malicious programs into the institution's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, by the Acceptable Use Policy.
- No lab shall provide production services. Production services are defined as ongoing and shared business-critical services that generate revenue streams or provide customer capabilities. These should be managed by the ICT Director.
- By the Data Classification Policy, information that is marked as institutional Highly Confidential, or Restricted is prohibited on lab equipment.
- Immediate access to equipment and system logs must be granted to members of the InfoSec Committee, the Network Operations Team, and the End User (Faculty and Students) upon request. The computer laboratory facility equipment, it is restricted to be utilized outside the school premises by the Acceptable Use Policy.
- InfoSec Committee will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.
- Only Faculty with approved Laboratory schedules are allowed to conduct classes during the laboratory period with the assistance of the Computer Lab Technicians.
- No Computer Laboratory Classes shall be conducted without the scheduled and assigned Faculty.
- Every Faculty and students are required to log in and rate to the local ICARE.edu.asscat.ph. For monitoring and laboratory utilization records.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Internal Lab Security Requirements.
- The Network Operations Team must maintain a firewall device between the institutional production network and all lab equipment.
- The Network Operations Team and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.
- The Network Operations Team must record all lab IP addresses, which are routed within ASSCAT networks management.
- Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.
- All traffic between the institutional production and the lab network must go through a firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.
- Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed as adding multiple firewall layers, the application of the segmentation multi-layered defense and even auditing firewall performance.
- Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the institutional network and/or non-ASSCAT networks. These activities must be restricted within the lab.
- Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.
- InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls, and network peripherals.
- Lab-owned gateway devices are required to comply with all ASSCAT product security advisories and must authenticate against the Institutional Authentication servers.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- The provided password for all lab-owned gateway devices must be different from all other equipment passwords in the lab. The password must be by ASSCAT's Password Policy. The password will only be provided to those who are authorized to administer the lab network.
- In labs where non-ASSCAT personnel have physical access (e.g., training labs), direct connectivity to the institutional production network is restricted. Additionally, no confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the institutional production network only if authenticated against the Institutional Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.
- Lab networks with external connections are prohibited from connecting to the institutional production network or other internal networks through a direct connection, wireless connection, or other computing equipment. Unless required or needed, a crafted network architecture should be presented/created.

## Related Standards, Policies, and Processes

- Acceptable Use Policy
- Classification of Information Policy
- Access Rights and Control Policy



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## IX. DATA CENTER SECURITY POLICY

### Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership, and configuration management are all about doing the basics well.

### Purpose

The purpose of this policy is to establish standards for Data Center and the base configuration of internal server equipment that is owned and/or operated by ASSCAT. Effective implementation of this policy will minimize unauthorized access to ASSCAT's proprietary information and technology.

### Scope

All employees, contractors, consultants, temporary and other workers at ASSCAT and its campuses must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by ASSCAT or registered under the ASSCAT-owned internal network domain.

This policy specifies requirements for equipment on the ASSCAT network and Data Center.

### Policy

#### General Requirements

Authorized personnel only may enter the ASSCAT Data Center. Authorized personnel must be registered in the Biometrics or a Card that allows them to access the Data Center.

General specifications of authorized personnel:

- College President
- Vice-Presidents
- Deans
- DTC Director
- MIS Personnels
- All personnel must sign in and out of the data center. The sign-in/sign-out process will record the time and date of entry and exit, as well as the purpose of the visit.
- All authorized personnel must surrender any electronic devices upon entry in the data center.
- The ITO must escort all visitors to the data center. Visitors must be escorted at all times while they are in the data center.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Allowed Visitors must have approved access by the College President or DTC Director for security monitoring and validation purposes only.
- All internal servers deployed at ASSCAT must be monitored by the Information Technology Officer (ITO) who is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and monitored by the ITO.
- Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the InfoSec Committee. The following items must be met:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the institutional management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedures
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.
- The Data Center must have a standardized and secured architectural layout of servers, workstations, and electrical equipment.
- Specify simple and proper Data Center and Network Connection access and utilization to avoid misconfigurations and confusion.
- The ITO shall identify key indicators for data and server security breaches.

## Data Center Facility and Network Connection

- New Data Centers require a business justification and VP-level approval from the business unit. Changes to the connectivity or purpose of an existing Data Center must be reviewed and approved by the InfoSec Committee.
- The Data Center must be in a separate room, cage, or secured lockable rack with limited access. In addition, the ITO must maintain a list of who has access to the equipment and a monitoring tool for the use of access and the purpose of visit.
- The Production Servers must not be directly connected to internal networks, logically through a wireless connection, or a multi-homed machine.
- A firewall device between the Production Servers and the Internet connection must be implemented. Firewall devices must be configured based on the least



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

privileged access principle. Cross-connections that bypass the firewall device are strictly prohibited.

- Implementation of robust restriction of entry for unauthorized access both physically and remotely.
- Data Center facilities must implement surveillance systems to safeguard against theft, sabotage, and unauthorized access.
- The Data Center must have continuous monitoring and control of entry points.
- The Data Center must adhere to the environmental hazard prevention and preparedness policy according to the stipulated disaster recovery plan policy.
- The implementation of the disaster risk recovery plan protocol must be established immediately upon approval of the incident commander.
- Secure backup power supply (diesel generators and/or battery backups if needed) and ensure quarterly monitoring.
- Establish procedures for incident reporting and proper response policy.
- The ITO shall identify key indicators for data and server security breaches.

## Configuration Requirements

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least-required access to perform a function. Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled, secured environment.
- Servers are specifically prohibited from operating from uncontrolled or unsecured cubicle areas.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security-related logs will be kept online for a minimum of 1 week.
- Daily incremental backups will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 6 months.

Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.
- Implement a centralized log management platform to monitor and analyze logs efficiently and effectively detect anomalies or any security breaches.
- Conduct regular security audits according to ISO/IEC 27001:2022 and any other regulatory requirements.
- The InfoSec team shall create, maintain, and monitor risk management plans for server security.

## Related Standards, Policies, and Processes

- Audit Policy
- Ensure compliance with Data Privacy Act of 2012 (Republic Act No. 10173).
- Ensure anti-theft locking mechanisms and protocols to prevent equipment or tool loss.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## X. DATABASE CREDENTIALS CODING POLICY

### Overview

Database authentication credentials are a necessary part of authorizing applications to connect to internal databases. However, incorrect use, storage, and transmission of such credentials could lead to the compromise of very sensitive assets and be a springboard to wider compromise within the institution.

### Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of the institution's networks.

Software applications running in the institution's networks may require access to one of the many internal database servers. To access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

### Scope

This policy is directed at all system developers and/or software engineers who may be coding applications that will access a production database server on the institutional Network and Cloud Server. This policy applies to all software (programs, modules, libraries, or APIS that will access the institution, a multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.

### Policy

#### General

To maintain the security of the institution's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text or easily reversible encryption. Database credentials must not be stored in a location that can be accessed through a web server. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to the date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Specific Requirements

### Storage of Data Base Usernames and Passwords

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be word-readable or writeable.
- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Passwords or passphrases used to access a database must adhere to the Password Policy.

### Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, database user names and passwords must be read from the file immediately before use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

### Access to Database Usernames and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Program database passwords are system-level passwords as defined by the Password Policy.
- Developer groups must have a process to ensure that database passwords are controlled and changed by the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Users and/or software accessing sensitive data must be subjected to proper access control and should not be able to perform privileged operations that are out of the scope of said user and/or software.

## Related Standards, Policies, and Processes

Password Policy



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XI. DISASTER RECOVERY PLAN POLICY

### Overview

A disaster recovery plan offers a crucial competitive advantage, even though disasters may seem infrequent. The institutional policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could potentially cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

### Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by the institution that will describe the process of recovering IT Systems, Applications, and Data from any type of disaster that causes a major outage.

### Scope

This policy is directed to the Digital Transformation Center which is accountable for ensuring the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirements around what goes into the plan or sub-plans.

### Policy

Developing or crafting policies for disaster recovery plan policies for server data disasters involves a structured approach to ensure an effective response to and recovery from unexpected data loss or system failures. Here are the key policies.

#### Data Backup Policy:

- Regularly schedule and perform backups of all critical data using data mirroring.
- Define backup frequency, retention periods, and storage location
- Ensure backups are tested periodically to verify data integrity and recovery processes.

#### Data Retention Policy:

- Establish guidelines for how long different types of data should be retained.
- Align data retention with regulatory requirements and business needs.
- Specify procedures for securely deleting data that is no longer needed.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## **Disaster Recovery Policy:**

- Define a comprehensive disaster recovery plan outlining steps to recover data and restore operations in case of a disaster.
- Identify critical systems and data, prioritize recovery efforts, and establish recovery time

## **Data Security Policy:**

- Implement security measures to protect data from unauthorized access, alteration, or destruction
- Define access controls, encryption standards, and monitoring procedures.
- Educate employees on security best practices and enforce compliance.

## **Incident Response Policy:**

- Establish protocols for responding to data loss incidents or breaches.
- Define roles and responsibilities of incident response team members.
- Outline steps for containing, investigating, and recovering from data disasters

## **Compliance Policy:**

- Adhere to relevant data protection regulations and industry standards. Regularly audit and review compliance with policies and legal requirements.
- Maintain documentation to demonstrate compliance efforts.

## **Training and Awareness Policy:**

- Provide regular training to employees on data protection policies and procedures.
- Foster a culture of data security awareness and accountability throughout the organization.

## **Testing and Evaluation Policy:**

- Conduct regular tests, simulations, or audits to assess the effectiveness of data disaster policies and procedures.
- Incorporate lessons learned from tests into policy revisions and improvements.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XII. EMAIL POLICY

### Overview

Electronic mail (email) is a primary means of communication both within the institution and externally. It allows quick and efficient conduct of business, but if used carelessly or unlawfully, it carries the risk of harm to the College and its community members.

### Purpose

The purpose of this policy is to describe the permitted uses of Institutional email. This policy is not meant to supersede or replace but should be read together with other Institutional policies. The Information Security Policy contains detail that is relevant to the use of email.

### Scope

This policy covers the appropriate use of any email sent from the institutional email address and applies to all employees, students, vendors, and agents operating on behalf of the institution.

### Policy

#### Ownership

- Employees, students, and authorized users: institutional email services must be used in a responsible, professional, effective and lawful manner.
- All accounts maintained on the institution's email systems are the property of this institution.
- The use of Institutional email services including the sending and forwarding of emails must comply with this Procedure, the Information Security Policies and other relevant Institutions' rules, policies and procedures.
- Institutional email accounts should be used for sending all institutional-related email communications both internally and to external organizations.
- The institution uses email as the primary method of communication with employees and students including urgent and time-critical information and announcements. Employees and students are required to check their Institutional email account on a frequent and consistent basis and respond to calls to action on time.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- All emails sent from Institution staff email accounts must be classified according to the Classification of Information Policy based on information contained within the email body and/or attachments. See the confidential and restricted emails section for more additional information.
- A disclaimer will automatically be attached to all outgoing emails from Institutional email accounts. This disclaimer must not be altered or interfered with in any way.
- After an employee and student separates from the institution, they are granted a 7-day window to transfer personal documents to their designated personal storage, whether physical or cloud-based. After this period, access to institutional email accounts will be discontinued. It is the employee's responsibility to ensure any necessary information to maintain business operations is handed over to their managers or teams before departure.
- Requests for delegate access to another employee's mailbox can be made through the DTC Office and require appropriate approval from the mailbox owner.
- Requests to delegate mailbox access to another employee when leaving the institution require approval from the mailbox owner and their supervisor or manager.
- Emails can be sent on behalf of another user as long as the user has given the appropriate approval and permissions.
- Emails sent from the institutional email accounts must not contain customized backgrounds. Backgrounds should remain as a default that is provided by the email applications.

## Unauthorized Actions

The following actions are not allowed when sending or forwarding emails:

- Using material that constitutes an infringement of copyright. Refer to the institution's Intellectual Property Rights Policy to determine what third-party material can be used.
- Defaming an individual, organization, association, company, or business.
- Communications that are obscene, offensive, or involve the use of illegal material, including the use or transfer of material of a sexual nature.
- Breaching an institution's policy, procedure, statute, or regulation.
- Directly or indirectly interfering with or conflicting with lawful Institution business.
- Intentionally bringing the institution or its officers into disrepute.
- Sending unsolicited and unauthorized global or commercial email messages.
- Forging or attempting to forge email messages.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- The forwarding of nuisance emails such as chain letters, junk mail, jokes, and frivolous attachments is strongly discouraged.

## Personal Use

Institutional email accounts are provided for academic and Institutional business operations. The institution allows the reasonable use of email for personal use under the following conditions:

- Personal use of email should not interfere with work responsibilities.
- Personal use of email does not interfere with the performance of the institution's network services.
- Personal emails must adhere to the Information Security Policies and associated procedures.
- Must not be used to run a private business whether for-profit or not-for-profit.
- Forwarding Institutional emails to personal email accounts, where permitted, is subject to delivery issues and should be avoided.

## Email Spam and Phishing

- Employees, students, and other authorized users of institution's email service should make themselves aware of educational activities and resources provided by the College to help identify potential cybersecurity threats and how to prevent them.
- Emails received that contain suspicious content, unexpected attachments or web links should not be opened and should be reported to the DTC Office.
- The institution will never ask for account details or in an email or ask users to validate their passwords through email links (phishing).
- Sharing passwords with others is prohibited and individual users may be held responsible for all actions including any infringement carried out by a third party given access to their accounts.
- Employees or students who believe they may have responded to a phishing email must immediately report to the DTC Office.
- Sending or forwarding a phishing email or an attachment or link that contains a virus is prohibited. Employees and students at institution-undertaking research or awareness campaigns may send emails containing such materials provided that it demonstrably refers to their area of research and is done so in a responsible manner and by any legislative requirements.
- The sending of unauthorized and unsolicited global or commercial email transmissions (spam) is not allowed.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Confidential and Restricted Emails

- Use the “bcc” function when mass sending emails to conceal the recipient email addresses from each other. This will provide an added layer of protection that reduces the risk of accidental data exposure.
- Emails containing confidential or restricted information or attachments must be classified appropriately according to the Classification of Information Policy.
- When sending or forwarding emails containing information or attachments classified as confidential or restricted to external organizations, the email should be signed and encrypted using an approved encryption method. These can include encryption features in WinZip. Passwords should be provided to the recipient using another form of communication such as phone or text message.
- Emails and sharing of documents via Google Drive must have user-level credentials according to their functions.

## Monitoring and Audits

- Emails may be monitored for the operational integrity of the Institutional Infrastructure and/or to comply with legal or regulatory requirements.
- The institution has the right to access and conduct audits on emails sent and received from Institutional email accounts as well as email records retained in college archive systems as part of the Information Security Policy.
- If there is evidence that a student or employee is not adhering to institutional policies or procedures, the institution reserves the right to take disciplinary action, including termination of access to institutional systems and services and/or legal action.

## Retention of Emails

- All email records from Institution email accounts will be retained for ten (10) years. All of the Office of the President, Vice Presidents, and Records Unit's email records will be retained indefinitely.
- Any exemption to the email retention period must be approved by the DTC Director, Records Officer Head/OIC, and Office of the President.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XIII. ENDPOINT DEVICES POLICY

### Overview

Any information stored on, processed by or accessible via user endpoint devices should be protected. Endpoint devices refer to any computing device that is connected to a network and communicates back and forth with a network. These devices include but are not limited to computers, laptops, smartphones, tablets, servers, security cameras, and any other device that can send or receive data over a network.

### Purpose

To protect information against the risks introduced by using user endpoint devices. This policy addresses the risk by establishing the responsibilities of users and the DTC to maintain the security of data that is stored, accessed, or transmitted via endpoint devices.

### Scope

This policy applies to all employees, students, contractors, vendors, and agents with ASSCAT-owned mobile devices. This policy covers all computers, servers, smartphones, tablets, and other computing devices operating within ASSCAT.

### Policy

#### Information Handling and Classification:

- Types of Information: Users should only handle, process, store, or support information authorized for their roles and security clearance.
- Classification Levels: User endpoint devices should only handle information up to their designated classification level (e.g., Confidential, Unclassified).
- Sharing and Transfer: Information sharing and transfer must comply with institutional policies and relevant regulations.

#### Registration of User Endpoint Devices:

- All user endpoint devices, both institutional-owned and personal (BYOD), must be registered before connecting to the network.
- The registration process includes device type, owner, operating system, security software, and classification level.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Physical Protection:

Users are responsible for the physical security of their devices, including:

- Implementing strong passwords and encryption.
- protect endpoint devices from unauthorized use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use.
- Do not leave devices carrying important, sensitive, or critical business information unattended.
- Use devices with special care in public places (lobby, corridors), open offices, meeting places, and other unprotected areas (e.g. avoid reading confidential information if people can read from the back, use privacy screen filters);
- Reporting lost or stolen devices immediately to the Digital Transformation Center (DTC).
- Physically protect user endpoint devices against theft (e.g. in offices, function halls, student's shed, lobby, corridors, and other meeting places)

## Software Installation Restrictions:

- Only authorized and licensed software may be installed on user endpoint devices.
- Installation of unreliable software requires approval from the DTC department.
- The ASSCAT System administrators may remotely manage and restrict software installations.

## User Endpoint Device Software Requirements:

- Devices must run approved operating systems and applications with updated versions.
- Active automatic updating of software and security patches is mandatory.

## Connection to External Networks:

- Connection to public networks or information services outside of the institution is prohibited unless explicitly authorized for essential purposes.
- The use of personal firewalls and VPNs is mandatory when connecting to external networks.
- For additional information, refer to *Remote Access and Remote Access Tools Policies*.

## Access Controls:

- Access to information and systems is granted on a need-to-know basis using multi-factor authentication. Please refer to
- Only authorized users shall be granted access to endpoint devices based on their role and responsibilities within the institution.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Access control measures, including strong authentication mechanisms shall be implemented to prevent unauthorized access and unauthorized use of endpoint devices.
- All access attempts and activities on endpoint devices shall be logged and monitored to detect and respond to any suspicious or unauthorized behavior.
- User accounts with appropriate permissions are essential.
- For additional information, refer to *Access Control Policy*.

## **Storage Device Encryption:**

- All removable storage devices and internal storage on user endpoint devices must be encrypted.
- Organization-approved encryption solutions are mandatory.

## **Protection against Malware:**

- Updated antivirus and anti-malware software must be installed and actively running.
- Regular security scans are mandatory.
- Reporting of suspicious activity is required.

## **Remote Disabling, Deletion, and Lockout:**

- The DTC has the authority to remotely disable, delete, or lock devices in case of security breaches, loss, or theft.
- Users must be informed about this capability.

## **Backups:**

- Regular backups of critical data on user endpoint devices must be performed.
- Backups should be stored securely off-site.
- Google Workspace's drive backup using an institutional account is highly recommended.

## **Usage of Web Services and Web Applications:**

- Use of authorized web services and web applications is permitted for work purposes.
- Downloading of unauthorized content is prohibited.

## **End User Behavior Analytics (EUBA):**

- EUBA may be implemented to monitor user activity for potential security risks.
- Users must be informed about EUBA practices.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Removable Devices:

- Use of unauthorized removable devices is prohibited.
- The DTC may disable physical ports like USB ports if necessary.

## Partitioning (if applicable):

- If supported, users may partition their devices to separate organizational information from personal data.

## Related Standards, Policies, and Processes

- Data Protection Standard
- Access Control Policy
- Remote Access
- Remote Access Tools



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XIV. INFORMATION TRANSFER POLICY

### Purpose

To maintain the security of information transferred within an organization and with any external interested party. To ensure that restricted information managed by various units and offices is protected from unauthorized transfer or disclosure.

### Scope

This policy states the minimum requirements for Information transfer or disclosure via electronic transfer, physical storage media transfer, and verbal transfer. This applies to all employees, students, and any third party that processes the institution's information.

### Policy

- The transfer or disclosure of personal data must be limited within the institution or personnel whose official functions warrant the disclosure or transfer of such data for legitimate purposes only.
- Before information is transferred through any channel, the sender must appropriately identify the individual who will receive the information. The recipient must be made aware of any duty of confidentiality and legal obligations when the information is sent.
- Always label transferred information with the appropriate level, "CONFIDENTIAL" or "RESTRICTED".

### Electronic Transfer

- In sending an email, label the subject header Confidential and/or RESTRICTED as appropriate.
- "CONFIDENTIAL" and "RESTRICTED" information shall only be transferred if necessary and for a legitimate purpose. The transfer should be avoided if possible and the quantity of data transferred shall be the minimum necessary.
- "CONFIDENTIAL" and "RESTRICTED" information shall be protected by a password before opening the document.
- Remote connections shall always be protected by a password and must be accessible to a specific user and level of accessibility.
- Transferring information using a public network is prohibited. The sender shall use a secured network connection outside the perimeter of the institution before accessing and sending any information.
- Transfer of information via email and Google Drive using an Institutional Account is advised. Provided that only appropriate users are allowed to access specific information with an applicable level of accessibility.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Information shall not be transferred or exchanged with other organizations unless a valid business reason exists.
- Employees and other interested parties shall not send short message service (SMS) or instant messages with critical information since these can be read in public places (and therefore by unauthorized persons) or stored in devices that are not adequately protected.

## **Physical storage media transfer**

- Only authorized and reliable couriers agreed by management shall the physical information be transported and shall be given strict instruction to hand over the document to the identified recipient only.
- “CONFIDENTIAL” and “RESTRICTED” information shall be labeled and sealed in the envelope, “To be opened only by the addressee” and log the transfer. There shall always be a named individual recipient
- The recipient shall be contacted to confirm they are on stand-by and again to confirm they have received the communication.
- The sender is responsible for controlling and notifying transmission, dispatch, and receipt of information.

## **Verbal Transfer**

- Information shall be kept out of earshot of unauthorized personnel.
- Personal Identifiable Information shall not be discussed on telephones that have hands-free capability unless they are located in a single-user office and only those persons who need the information are present.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XV. INTELLECTUAL PROPERTY RIGHTS

### Purpose

To ensure compliance with legal, statutory, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary products.

### Scope

This includes but is not limited to computer software licenses, devices, manuals, books, articles, or other documents, other than those permitted by copyright law or the applicable licenses.

### Policy

- Ensure that only authorized software and licensed products are installed and utilized by employees and students.
- Software installation must be only through known and reputable sources, to ensure that copyright is not infringed upon.
- Installation of devices and software applications must be by the allowed number of resources indicated in the purchased license.
- Time-based licensing should be monitored by the end-users and must be renewed according to its usage.
- No copying, in full or in part, standards, books, articles, reports, source code, software, or other documents, other than permitted by copyright law or the applicable licenses.
- Research publications should undergo plagiarism application checking.
- And other policies indicated in institutional Research and Development Intellectual Property Policies



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XVI. LABELLING OF INFORMATION POLICY

### Purpose

To facilitate the communication of information classification and support automation of information processing and management.

### Scope

Information labeling covers information and other associated assets in all formats. Labeling of non-confidential information will be omitted to reduce workloads. In addition, documents provided and controlled by other agencies are not included.

### Policy

- In this policy, labels of information shall refer to the categories under the Information Classification Policy of this document.
- An employee can access information classified as “RESTRICTED” or “CONFIDENTIAL” in their work, only if their job or role within the institution justifies this or if they are granted permission from the proper authority. Information shall not be kept where only one individual can access it.
- Emails are always classified as “CONFIDENTIAL” or “RESTRICTED”, regardless of their content.

### Digitized Data

#### *Metadata*

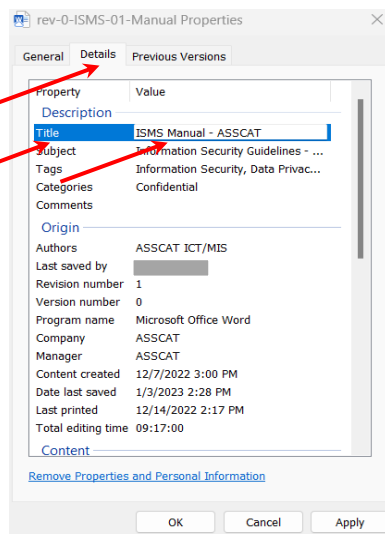
Digital information including In-housed Information Systems may use metadata to identify, manage, and control information.

#### How to Add Metadata to a document

- Open up your computer’s folder containing the document, image, or video file.
- Windows users: Right-click on the file, and select Properties. For Mac users: Control-click, and select “Get Info” (or press command + i on your keyboard).
- In the window that appears, you can change the value to specific properties.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY



Set the following Properties:

Property	Value
Title	File/Image/Video-specific keyword - ASSCAT
Subject	File/Image/Video-specific - ASSCAT
Tags	File/Image/Video-specific keyword; ASSCAT
Manager	Name of the institution
Authors	ASSCAT – Specific Office
Version Number	Numerical

## *Headers and Footers*

Any documents created by the institution must contain the following in the footer or header.

- Title of the Document
- Institutional Logo
- Name of the institution
- Name and logo of the Partner Institution (*if applicable*)
- Information Classification (Confidential, Restricted, Internal, or Public)
- Page Number
- Document Number, revision number, and effectivity date (*for ISO-controlled documents*)
- The footer must contain the Information Classification for Confidential and Restricted.

## *Watermarking*

Applying digital security watermarks to sensitive documents to prevent data loss, misuse, and unauthorized sharing.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Below are the following documents but are not limited to shall apply a digital security watermark.

- Intellectual Property
- Academic Records
- Building Plans
- Legal Contracts
- Human Resources documents
- Financial Documents (*excluding COA and DBM controlled forms*)
- Manuals
- Watermarks Guidelines:
- Use the institutional logo for User Manuals, Instructional Materials, or as needed.
- Indicate the information classification to the Confidential and Restricted for documents as needed

## *Physical Data*

### **Physical Labels**

Labelling of information using physical labels shall only be applied if the documents created or received are already printed bearing no label. It shall be implemented in all units or offices whenever applicable following these formats:

1. Upon creation or receipt of the document, the author/receiver will need to classify the document based on the appropriate classifications of "Confidential", or "Restricted". Any information that is not specifically labelled are automatically considered "Public".
2. Attach the physical label to the document using the following format, whichever is best suited:
  - a. Adhesive Label. This can be put on each page of the document or if the multiple documents are enclosed in a folder or envelope. Labels should have the following specifications:
    - Font – Arial (Bold)
    - Font size – 18Each label should be printed on white bond paper and pasted at the upper right of the folder cover or envelope.
  - b. Spine Labels. This can be ideal for documents organized in a binder. Specifications for adhesive labels shall also be followed.

### **Rubber-stamps**

A stamp on the physical document is another form of information labelling. The owner of the information shall be responsible for putting the appropriate stamp on each page of the document.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XVII. PASSWORD AND AUTHENTICATION POLICY

### Purpose

Passwords are fundamental to information security, shielding user accounts and safeguarding ASSCAT's network and information in Information Systems and Google Drives. Weak passwords leave them vulnerable. Therefore, all ASSCAT employees and students must adhere to password policies.

### Scope

The scope of this policy includes all employees and students with institutional accounts or any access requiring a password provided by ASSCAT. This also includes external information systems and other services provided to ASSCAT, where ASSCAT users are considered end-users.

### Policy

#### General

- All system-level passwords (e.g., root, network admin, information system administrators, servers, etc.) must be changed at least every 90 days.
- All user-level passwords (e.g., emails, institutional accounts, desktop computers, social media accounts owned by ASSCAT, etc.) must be changed at least every 90 days.
- Password options on all servers must require passwords to have a minimum of 8 characters, including a combination of uppercase, lowercase, numbers, and symbols.
- Default passwords must be changed to strong passwords after the first login.
- Reusing previous passwords is not allowed.
- 2-step verification is enforced for institutional accounts for employees and students. The users may choose from the following verification methods:
  - Security keys
  - Google prompt, text message, or phone call
  - Google Authenticator app
  - Backup codes

#### *Guidelines for Construction of Passwords*

A strong password can be memorable but nearly impossible for someone else to guess.

- Avoid using "ASSCAT" or an Office in ASSCAT or any derivation
- Make password unique



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 55 of 87

- Use a different password for each of the important accounts, like email and online banking applications.
- Reusing passwords for important accounts is risky. If someone gets the password for one account, they can access the email, address, and even the money in bank accounts.

## Use letters, numbers & symbols

- Passwords with different types of symbols might be more difficult for people to guess but also might be harder to remember.
- Combine different types of characters
- Use a mix of alphanumeric characters (letters and numbers) and symbols:
  - Uppercase (capital) letters. Examples: A, E, R
  - Lowercase (small) letters. Examples: a, e, r
  - Numbers. Examples: 2, 6, 7
  - Symbols and special characters. Example: ! @ & \*

## Recommendations & examples

- Replace letters with numbers & symbols: Choose a word or phrase and use numbers and symbols instead of some letters. Examples:
- "Spooky Halloween" becomes "sPo0kyH@ll0w3En"
- "Later gator" becomes "L8rg@+0R"
  - Abbreviate a sentence: Come up with a sentence and use the first letter of each word.

Example:

"Uncle Peter always ate chocolate-covered everything"  
becomes "uP@8cCe!"

## Avoid personal information and common words

### Don't use personal information

Avoid creating passwords from info that others might know or could easily find out. Examples:

- Your nickname or initials
- The name of your child or pet
- Important birthdays or years
- The name of your street
- Numbers from your address

### Don't use common words & patterns



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Avoid simple words, phrases, and patterns that are easy to guess.

Examples:

- Obvious words and phrases like "password" or "letmein"
- Sequences like "abcd" or "1234"
- Keyboard patterns like "qwerty" or "qazwsx"
- Any examples in this article, like "sPo0kyH@ll0w3En" or "uP@8cCe!"

## Password Protection Standards

All passwords are to be treated as confidential ASSCAT information. The following policies are to be taken to protect the passwords.

- Users must use a separate, unique password for each of their work-related accounts.
- Don't reveal a password over the phone, or an e-mail message/chat with ANYONE.
- Don't share a password with family members
- Don't reveal a password to co-workers while on leave
- Don't use the "Remember Password" in any applications or browsers.
- Don't write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system without any encryption.

## Application Development

- Application developers must ensure that their programs contain the following security precautions:
  - Applications must support the authentication of individual users, not group
  - Applications must not store passwords in clear text or any easily reversible form.
  - Applications must not transmit passwords in clear text over the network.
  - Applications must provide some sort of role management, such that one user can take over the functions of another without having to know the other's password.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XVIII. PROJECT MANAGEMENT POLICY

### Overview

Project management policies and procedures provide 'rules' and precedents so that a project's management is not haphazard or inconsistent. Protecting sensitive data, intellectual property, and systems from unauthorized access, use, disclosure, disruption, modification, or destruction is crucial for ensuring project integrity, meeting deadlines, and delivering desired outcomes.

### Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle as well as to promote consistency and better control of projects, thereby reducing risks and increasing project success.

### Scope

This can be applied to any type of project regardless of its complexity, size, duration, discipline, or application area. These include but are not limited to information system development, project development plans, external projects funded by partner institutions, and research projects.

### Policies

#### *General Projects*

- Regardless of their present employment status or past connection to the institution, an employee shall not, at any time or in any manner, directly or indirectly disclose or communicate to any person, firm, or corporation any information of any kind concerning any matters affecting or relating to the business of the institution, including but not limited to the names of its partners, employees, and students, or any other information concerning the business, its operations, strategies, plans, processes, or other data, regardless of whether such matters would be deemed confidential, material, or important.
- All work output content associated with the Projects, including but not limited to images, graphic user interfaces, source and object code, soft copies, documentation, and notes, shall be the exclusive property of the institution. Regardless of whether such work output is created on privately owned equipment, the institution shall retain title to all intellectual property rights relating to the Projects, including but not limited to copyrights, trademarks, patents, and trade secrets.
- Design plans, contracts, requirements, blueprints, and any other project-related documents must be kept confidential. Project managers are responsible for



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

ensuring the confidentiality, integrity, and availability of these documents in any format, even in the event of security threats.

- Throughout the project lifecycle, web filtering, and computer antivirus activation act as essential safeguards to protect information and information processing facilities from malware threats.
- A proper change management process shall be followed throughout the project lifecycle to address any changes that arise. This includes thorough documentation and turnover of requirements to ensure all stakeholders are informed of the change, its rationale, and the steps involved in its implementation.

## Information System Development

- Information System Development Procedure and Design Plan must be followed as guidance on making decisions during the project life cycle.
- Virtual Local Area Network for system development and deployment must be separate and not accessible to the other network of the college to prevent unauthorized access.
- Environments for development, testing, and production environments must be separated to reduce risks and threats of unauthorized access or changes to the operational environment.
- Developers are only allowed to access the development and testing environments. For deployment, the assigned server administrator or DevOps is responsible for continuous integration and development, automated server deployment, and monitoring.
- All Source codes must be stored in a private code versioning control repository managed by the institution. Inactive developers will be automatically removed from the assigned repository.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XIX. REMOTE ACCESS POLICY

### Overview

Remote access to our institutional network is essential to maintain our ICT Personnel's productivity, but in many cases, this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our institutional network. Some service providers also use remote access connections during maintenance activities.

### Purpose

The purpose of this policy is to define rules and requirements for connecting to ASSCAT's network from any host. These rules and requirements are designed to minimize the potential exposure to ASSCAT from damages which may result from unauthorized use of ASSCAT resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical ASSCAT internal systems, and fines or other financial liabilities incurred as a result of those losses.

### Scope

This policy applies to all ASSCAT employees, students, contractors, vendors, and agents with an ASSCAT-owned or personally-owned computer or workstation used to connect to the ASSCAT network. This policy applies to remote access connections used to do work on behalf of ASSCAT, including network configuration, server management, and system administration. This policy covers any technical implementations of remote access used to connect to ASSCAT networks.

### Policy

It is the responsibility of ASSCAT employees, students, contractors, vendors, and agents with remote access privileges to ASSCAT's institutional network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ASSCAT.

General access to the Internet for recreational use through the ASSCAT network is strictly limited to ASSCAT employees, students, contractors, vendors, and agents (hereafter referred to as "Authorized Users"). When accessing the ASSCAT network from a personal computer, Authorized Users are responsible for preventing access to any ASSCAT computer resources or data by non-authorized users. Performance of illegal activities through the ASSCAT network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for any consequences of misuse of the Authorized User's access. It is the responsibility of the end-users to monitor the vendors, contractors, and agents with access privileges during a remote access connection. For further information and definitions, see the *Acceptable Use Policy*.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Authorized Users will not use ASSCAT networks to access the Internet for outside business interests.

## Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.
- Authorized Users shall protect their login and password, even from family members.
- While using an institutional-owned computer to remotely connect to the institutional network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except personal networks that are under their complete control or the complete control of an Authorized User or Third Party.
- All hosts that are connected to the institution's internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers.
- All third-party, vendor, and service providers' remote access connections must be approved by the ICT Unit Head and must be monitored by the Network or System Administrators during the entire access.
- Personal equipment used to connect to the institution's networks must meet the requirements of institution-owned equipment for remote access as stated in the *Remote Access Tools Policy*.
- The remote access user also agrees to and accepts that his or her access and/or connection to the institution's networks may be monitored to record dates, times, duration of access, and other relevant data to identify unusual usage patterns or other suspicious activity.

## Related Standards, Policies, and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods and acceptable use of ASSCAT's network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Remote Access Tools Policy*



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XX. SOFTWARE INSTALLATION POLICY

### Overview

Allowing employees to install software on the institution's computing devices opens to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during the audit, and programs can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on equipment.

### Purpose

The purpose of this policy is to outline the requirements for installation software on institution-owned computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within the institution's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

### Scope

This policy applies to all employees, contractors, vendors, and agents with institution-owned mobile devices. This policy covers all computers, servers, smartphones, tablets, and other computing devices operating within the institution.

### Policy

#### General Policy

- The Employees must not install cracked or unlicensed software on institutional-owned computing devices operated within or outside the institution's network.
- Software requests must first be approved by the requester's manager and then be made to the Digital Transformation Center in writing or via email.
- Software must be selected and approved by the Information Technology Officer.
- The Digital Transformation Center will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

#### Authorize and Secure Software Sources

- Ensure that only authorized security software is installed on systems and maintain an inventory of approved security software to track installations.
- Obtain security software from trusted and reputable sources. Avoid downloading security software from unofficial or unknown websites.
- Verify that the security software is compatible with the operating system and other applications on the system.
- Check hardware requirements to ensure smooth operation.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Installation Procedure and Patch Management

- Follow vendor-provided installation guides and best practices.
- Configure settings according to security recommendations and organization policies.
- Immediately apply any necessary patches or updates to the security software after installation.
- Regularly check for and apply vendor-supplied patches to address vulnerabilities.

## Access Controls and Configuration

- Limit installation rights to authorized personnel on a need-to-install basis.
- Use the principle of least privilege to restrict access to security software configurations.
- Configure security software according to best practices and hardening guidelines.
- Disable unnecessary features and services to reduce the attack surface.
- Conduct testing after installation to ensure the security software functions as intended.
- Validate that the security software is detecting and blocking threats effectively.
- Maintain documentation of the installed security software, including version numbers, configuration settings, and deployment dates.

## Documentation and Training

- Document any exceptions or deviations from standard installation procedures.
- Provide training to system administrators and users on the purpose and use of the security software.
- Educate users on security policies related to the software and how it protects the organization.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXI. STORAGE MEDIA POLICY

### Purpose

To ensure only authorized disclosure, modification, removal, or destruction of information on storage media.

### Scope

Storage media including paper owned by ASSCAT containing confidential information. This policy covers its life cycle of acquisition, use, transportation, and disposal.

### Policy

#### *Removable storage media*

- Information Asset Owners are responsible for the confidentiality and integrity of information saved in storage media.
- Store all storage media in a safe, secure environment according to their information classification and protect them against environmental threats (such as heat, moisture, humidity, electronic field, or aging), according to manufacturers' specifications.
- Confidential information stored in storage media must be encrypted especially when sending it via the postal service or courier.
- Safely eject storage media after use.

#### *Secure reuse or disposal that contains confidential information*

- Reformat storage media before reuse.
- Dispose of the storage media by destroying, shredding, or securely deleting the content.
- Log the disposal of sensitive items to maintain an audit trail.

### Retention of Storage Media

This retention policy applies to all end-users or entities with access to storage media owned by the organization. Its objective is to ensure efficient management of storage media throughout its lifecycle while adhering to statutory or regulatory requirements.

- The retention period for storage media containing sensitive information must comply with external policies, such as those established by the National Archives of the Philippines, regarding data retention. Retention periods may vary depending on the type of data and its regulatory or operational requirements.
- All storage media should undergo sanitization (*the process of securely erasing data stored on various types of storage devices*), to be performed by authorized personnel. Sanitation



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

may be necessary during media transitions, such as when transferring it to someone with a different role, relinquishing it, or replacing it.

Different methods of storage media sanitation may be applied by the institution depending on its available resources:

- **Data wiping or overwriting:** This involves using software tools to overwrite the entire storage media with random data multiple times, making the original data unrecoverable.
- **Physical destruction:** This involves physically destroying the storage media using methods such as shredding, crushing, or degaussing (for magnetic media). Physical destruction ensures that the data cannot be recovered from the device.
- **Secure erase:** Some storage devices, particularly solid-state drives (SSDs), come with built-in secure erase functionality that allows for the complete and irreversible deletion of data stored on the device.

Storage media sanitation is performed when disposing of or repurposing storage devices to ensure that sensitive data cannot be accessed by unauthorized individuals. To prevent the unauthorized disclosure of organizational information when disposing of storage media, the organization shall adhere to specific guidelines regarding the disposal of defective storage devices stated in the Technology Equipment Disposal Policy.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXII. SUPPLIER RELATIONSHIP POLICY

### Purpose

To maintain an agreed level of information security in supplier relationships

### Scope

Acquisition of ICT resources, and maintenance conducted remotely or onsite by the service providers to termination of use and services.

### Policy

#### ***Non-Disclosure Agreement:***

A Non-Disclosure Agreement specified in the contract must be signed by the institution representatives and the External Provider to ensure a clear understanding of both parties' obligations to fulfill relevant information security requirements. This agreement should address:

The institution's confidentiality, integrity, availability, and information handling requirements.

#### ***Changes to Deliverables:***

- Any changes to the deliverables specified in the contract due to technological advancement must be discussed with the supplier and should be approved by the Head of the Procuring Entity (HOPE) which is the BOT.

#### ***Maintenance and Change Management:***

- The supplier shall have on-call technicians for maintenance.
- The supplier shall inform the institution especially the direct end-user of the project of any changes made, including:
  - Enhancements to current services offered
  - Development of any new applications and systems
  - Modifications or updates to the supplier's policies and procedures
  - New or changed controls to resolve information security incidents and improve information security
- The supplier shall also inform the institution of any changes in services, including:
  - Changes and enhancements to networks
  - Use of new technologies
  - Adoption of new products, newer versions, or releases
  - New development tools and environments
  - Changes to the physical location of service facilities
  - Change of sub-suppliers
  - Sub-contracting to another supplier



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## *Project Documentation and Termination:*

- Project Technical Documentation containing authentication and detailed project implementation must be provided by the supplier before the termination of the contract.
- The following activities must be conducted to ensure the secure termination of the supplier's relationship and completion of the projects:
  - De-provisioning of access rights
  - Information handling
  - Transfer of ownership of intellectual property developed during the engagement
  - Information portability in case of a change of supplier or insourcing
  - Records management
  - Secure disposal of information and other associated assets
  - Ongoing confidentiality requirement



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXIII. SYSTEM CHANGE MANAGEMENT POLICY

### Overview

Managing changes to an organization's IT infrastructure is crucial for maintaining stability, security, and efficiency. The System Change Management Policy offers a framework to effectively handle alterations in information systems, software applications, hardware, and associated components. Its goal is to minimize disruptions, mitigate risks, and ensure that changes align with the organization's objectives and compliance mandates.

### Purpose

The System Change Management Policy is designed to promote a structured and disciplined approach to managing changes within an organization's IT environment.

### Scope

This policy covers all changes to an organization's information systems, including but not limited to:

- Software Updates and Patches
- Hardware Upgrades or Replacements
- Configuration Changes
- Network Modifications
- Database Changes
- Security Policy Changes
- Application Development and Deployment

### Policy

#### General Policy Statement

- All the information systems changes must be planned, documented, tested, and approved before the implementation process shall be implemented.
- All the changes that may impact security, including but not limited to software updates, configuration changes, and hardware modifications, must undergo a formal review and approval of the formal change management process.
- A change management committee shall be created for planning, assessing, approving and implementing changes to information systems.
- The change management committee shall consist of authorized personnel specific to the process's hierarchical approval.
- Emergency changes must be documented and approved by the change management committee as soon as possible after the implementation with appropriate risk assessment and mitigation measures in place.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- All the changes must be approved and authorized by the change management committee and process owners before the implementation.
- All change management policy documents and all other referenced documents shall be controlled.
- All the Change Management Policy documents shall be made available to all employees covered in the scope, relevance, and or as necessary.
- All the Change Management documents shall be considered “confidential” and shall not be made available to unauthorized persons outside of the organization.
- The policy is applicable only for software and hardware changes or updates.

## Change Request Process

- The requester must formally request a change by processing for the approval of a Change Management Request Form.
- The requester has to justify their proposed changes.
- The requester must document all relevant details of changes, expected outcomes, and potential impact of the change process.
- The Change Management Committee shall plan and/or assess the potential impact of changes considering all dependencies.
- Communicate changes to relevant interested and/or involved parties.
- Involved parties have to approve the proposed changes together with the change management committee.

## Change Implementation

- Specify guidelines for carrying out changes, including rollback plans and communication strategies in adherence to the institution's policies and guidelines.
- Ensure adequate documentation of all changes for future reference
- Provide mechanisms for the proper implementation.
- The Change Management Team shall also decide on the level of priority in the change management process request as to the implementation and approval.

## Monitoring and Reporting

- Implement continuous monitoring of system changes to detect anomalies and performance issues.
- Require regular reporting on the status of ongoing and completed changes
- The system developers together with the end-users will conduct a risk assessment to check all the systems and processes affected by the proposed change.
- The Change Management Team shall provide recommendations and a list of any risk areas identified to ensure security compliance and mitigate risk factors.

## Training and Awareness

- Ensure that personnel involved receive appropriate training to understand their roles and responsibilities in maintaining the security of all information systems.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- The InfoSec Team shall conduct necessary training and awareness of the information systems, its security and change management implementation.
- Awareness initiatives must be implemented and shall promote a culture of security and encourage all employees to adhere to security policies and report any suspicious or unauthorized changes promptly to avoid security breaches.
- Enforce best practices for security policy compliance to all stakeholders in the organization.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXIV. SYSTEM DEPLOYMENT AND TEST POLICY

### Overview

System deployment refers to the process of releasing a new or updated software or hardware solution to the end users. It involves planning, testing, installation, configuration, training, and support activities that ensure the system meets the requirements and expectations of the stakeholders.

### Purpose

This policy aims for the systematized and standard deployment of the Data Processing System. The training of end-users, safeguarding the system from possible attacks, and determining the system security vulnerabilities.

### Scope

The policy applies to the staging and production deployment of the Data Processing System, and the functional, security, and performance testing. The policy also applies to the end users' training and the concerned office.

### Policy

Sensitive information should not be copied into the development and testing environments.

### Staging/Test Deployment and System Testing

- Testing should be performed in a test environment that matches the target production environment as closely as possible to ensure that the system does not introduce vulnerabilities to the organization's environment and that the tests are reliable
- The on-premise servers used for production must have a dedicated environment for testing.
- Secure configurations including operating systems, firewalls, and other security components.
- The on-premise test server running using a virtual machine must have the same environment as the production server whether it will be on another virtual machine or in AWS EC2 or any cloud server infrastructure.
- Conduct System security testing
- Performing penetration testing to identify insecure code and design
- Performing vulnerability scanning to identify insecure configurations and system vulnerabilities.
- Performing code review activities as a relevant element for testing for security flaws, including unanticipated inputs and conditions



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- The programmer must provide training to the end users and the concerned office.
- The concerned office should conduct Functional testing to ensure the system meets the requirements and expectations.
- The Information System Analyst and the Programmer should conduct the performance testing
- All determined security vulnerabilities, adjustments, and subject to change have to be addressed before the deployment to production.

## Production Deployment

- After the approval of System acceptance from the concerned office. The production deployment will follow
- A dedicated production environment is maintained on both the on-premise server and AWS EC2, and only authorized personnel are permitted to manage production tasks.
- Using End-to-End Security and Privacy Service Portfolio tools to improve security, and increase privacy.

Example tools are:

- Firewall
  - Intrusion Detect Protect
  - Vulnerability Assessment tool
  - Logs Management Events and Context Logs
  - Data Backup and Recovery
  - Security Information and Event Management (SIEM)
  - Configuration Management Database (CMDB)
  - Patch Management
  - Data Loss Prevention
  - PKI and Data/Host Encryption
- Major and Minor System flow changes have to undergo System testing and follow the System Change Management Policy.
  - Urgent Changes like bug fixes and a hotfix has to fill out a Report form for the changes and to be reviewed and tested by the Information System Analyst and the Programmer before being deployed to the production

## Related Standards, Policies, and Processes

- Computer Laboratory Security Policy
- Web Application Security Policy



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXV. SYSTEM DEVELOPMENT POLICY

### Overview

System applications are valuable to the institution because they solve some manual work, reduce operational costs by automating routine tasks, reduce human resources, increase or measure business productivity, improve efficiency by eliminating human errors via maintaining accuracy and reliability

### Purpose

This policy aims to establish the standard development for system security, scalability, and maintainability.

### Scope

The policy applies to the Development of the Data Processing Systems

### Policy

#### Project Development Team

- The project team shall be led by one project team leader. A Project Leader shall be a bonafide employee of the institution.
- The team leader shall consult and work with departmental heads, managers, and other stakeholders to develop team goals and delegate tasks to the appropriate team member. This includes the project execution and the identification of the project scope.
- The project team leader shall create and identify the composition of the project development team.
- Shall develop team schedules and assist in the successful onboarding and training of team members. Create and communicate a clear list of expectations and goals for team members to follow.
- The team members shall report and post updates on the task given. They are responsible for the completion of the task within the expected schedule.
- Project Prioritization
- The proposed project shall be evaluated and identified as to the needs of the institution. This includes the organizational goals, risk and financial availability for the project development.
- Information System Data and Functional Gathering
- Determine the platform to use based on the system requirements.
- Determine the information to be protected for data privacy.
- Secure Development Life Cycle
- Secure repositories for source code and configuration
- The administration access of the remote version control is on the MIS Head Officer or assigned personnel to administer the repository



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Separation of Development, Test, and Production Environment

Environment	Tools
Development	The development environment is on the Computer Programmer's workstation
Test	The test or staging environment is on the on-premise server
Production	The production environment is on the Microsoft AWS EC2 or designated on-premise server

Security requirements in the specification and design phase

The Information Analyst has to determine the security requirements for the system.

Examples are:

- Access restrictions
- Authorization of disposal of information and other associated assets and supported deletion method(s)
- Restriction to privileged access
- Logging
- Relevant legislation, regulations, and any contractual obligations regarding limitations of access to data services

## System Design

System Analysts formulate the system design according to the gathered requirements including:

- Time Tables
- Process Flowchart
- Data Flow Diagram
- ERD
- Network Layout
- Architectural Diagram
- Project cost table

## Secure Coding

follow the suggested practices specific to the programming languages and techniques

Examples are:

- Query Binding or using ORM
- Validate input fields
- Using the updated version of the development stack
- Pair programming, programs should be reviewed by the senior developer before the approval of the repository pull request.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited;
- Prohibiting the use of insecure design techniques (e.g. the use of hard-coded passwords, and unauthenticated web services)

## Data Masking

- Not granting all users access to all data, therefore designing queries and masks to show only the minimum required data to the user
- Masking of sensitive data from development set-up and system staging using these data masking methods:
- Substitution (changing one value for another to hide sensitive data)
- Nulling or deleting characters (preventing unauthorized users from seeing full messages);
- Encryption (requiring authorized users to have a key);
- Varying numbers and dates;
- Replacing values with their hash.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXVI. TECHNOLOGY EQUIPMENT DISPOSAL POLICY

### Overview

Technology equipment often contains parts cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, and other storage media contain various kinds of ASSCAT data, some of which are considered sensitive. To protect our institution's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion but is still accessible until it is overwritten by a new file. Therefore, special tools must be used to securely erase data before equipment disposal.

### Purpose

The purpose of this policy is to define the guidelines for the disposal of technology equipment and components owned by ASSCAT.

### Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within ASSCAT including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smartphones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, portable storage devices (i.e., USB drives), Network Attached Storage, printed materials.

All ASSCAT employees and affiliates must comply with this policy.

### Policy

#### Technology Equipment Disposal

- When Technology assets have reached the end of their useful life, they should be sent to the Disposal Committee for proper disposal.
- The Disposal Committee will securely erase all storage mediums according to current industry best practices.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting every disk sector of the machine with zero-filled blocks.
- No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).
- No computer equipment should be disposed of via skips, dumps, landfills, etc. Electronic recycling bins may be periodically placed in locations around ASSCAT. These can be used to dispose of equipment. The Disposal Committee will properly remove all data before final disposal.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing, or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- The Disposal Committee will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the DTC IT Support Technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

## Employee Purchase of Disposed Equipment

- Equipment is working, but reached the end of its useful life to ASSCAT, will be made available for purchase by employees.
- The system approved by the Disposal Committee will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the system stated in 4.2.2. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees or clients have an equal chance of obtaining equipment.
- The Finance and Disposal Committee will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with any equipment sold.
- Before leaving ASSCAT premises, all equipment must be removed from the Information Technology inventory system.

## Related Standards, Policies and Processes

- DENR Administrative Order No. 2001 - 34
- DAO 2001-34 Implementing Rules and Regulations of RA 9003
- Republic Act 9003 and its Implementing Rules DAO-2021-19 - Department of Environment and Natural and Resources
- DENR Administrative Order No. 20



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXVII. WEB APPLICATION SECURITY POLICY

### Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and that any vulnerabilities be remediated before production deployment.

### Purpose

This policy aims to define web application security assessments within the institution. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of the institutional services available internally and externally and satisfy compliance with any relevant policies in place.

### Scope

- This policy covers all web application security assessments conducted by any individual, group, or department to maintain the security posture, compliance, risk management, and change control of technologies in use in the institution.
- All web application security assessments will be performed by delegated security personnel either employed or contracted by the institution. All findings are confidential and will be distributed to persons on a “need-to-know” basis. Distribution of findings outside of the institution is strictly prohibited unless approved by the Chief Information Security Officer.
- Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented before the start of the assessment.

### Policy

Web applications are subject to security assessments based on the following criteria:

- **New or Major Application Release** – will be subject to a full assessment before approval of the change control documentation and/or release into the live environment.
- **Third Party or Acquired Web Application** – will be subject to full assessment after which it will be bound to policy requirements.
- **Point Releases** – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- **Patch Releases** – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- **Emergency Releases** – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Security Officer or an appropriate manager who has been delegated this authority.
- **Annual Review** – all applications will be subject to a full annual review in its entirety to review potential risks of functionality and/or architecture.
- All security issues that are discovered during assessments must be mitigated based on the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fixes and/or mitigation strategies for any discovered issues of medium risk level or greater.
- **High** – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken offline or denied release into the live environment.
- **Medium** – Medium risk issues should be reviewed to determine what is required to mitigate and schedule accordingly. Applications with medium-risk issues may be taken offline or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- **Low** – The issue should be reviewed to determine what is required to correct the issue and schedule accordingly.
- The following security assessment levels shall be established by the InfoSec committee or other designated organization that will be performing the assessments.
- **Full** – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any discovered.
- **Quick** – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- **Targeted** – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.
- The currently approved web application security assessment tools in use which will be used for testing are:
  - Nmap
  - Burpsuite
  - Sqlmap
  - Wpscan



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Zap
- Sqlninja
- jSQL Injection

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Operations Center team.

## Related Standards, Policies and Processes

- OWASP Top Ten Project
- OWASP Testing Guide
- OWASP Risk Rating Methodology



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXVIII. WIRELESS COMMUNICATION POLICY

### Overview

With the mass explosion of smartphones and tablets, pervasive wireless connectivity is almost a given in any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

### Purpose

The purpose of this policy is to secure and protect the information assets owned by the institution. The institution provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. The institution grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the institutional network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Committee are approved for connectivity to the network.

### Scope

All employees, contractors, consultants, temporary and other workers in the institution, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the institution must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the ASSCAT network or reside on the ASSCAT site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

### Policy

#### General Requirements

All wireless infrastructure devices that reside at the institution's site and connect to the network, or provide access to information classified as Confidential, or above must:

- Abide by the standards specified in the *Wireless Communication Standard*.
- Be installed, supported, and maintained by the DTC Technical Support Team.
- Use institutional-approved Password and Authentication Policy and infrastructure.
- Follow Acceptable Encryption Policy.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Do Not interfere with wireless access deployments maintained by other support organizations.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Lab and Isolated Wireless Device Requirements

- All lab wireless infrastructure devices that provide access to Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the institutional network must:
- Be isolated from the institutional network (that is it must not provide any institutional connectivity) and comply with the *Lab Security Policy*.
- Do Not interfere with wireless access deployments maintained by other support organizations.

## Wireless Device Requirements

- Wireless infrastructure devices that provide direct access to the ASSCAT institutional network, must conform to the Wireless Device Requirements as detailed in the *Wireless Communication Standard*.
- Wireless infrastructure devices that fail to conform to the Wireless Device Requirements must be installed in a manner that prohibits direct access to the ASSCAT institutional network. Access to the ASSCAT institutional network through this device must use standard remote access authentication.

## Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Wireless Communication Standard

### Wireless Network Security:

- All wireless networks must be secured with strong encryption protocols (e.g., WPA3) to prevent unauthorized access.
- Default SSIDs should be changed to unique names to avoid easy identification.

### Access Control:

- Wireless access points (WAPs) must be configured to use strong passwords or keys for access.
- Access to wireless networks should be restricted based on job roles and requirements.

### Guest Wireless Networks:

- Guest networks should be isolated from the internal network, with limited access to company resources.
- Guests must authenticate using a captive portal with terms of use and acceptable use policies.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## **Wireless Device Security:**

- All wireless devices (laptops, smartphones, tablets) must have up-to-date security software (e.g., antivirus, antimalware).
- Devices should use secure authentication methods (e.g., multi-factor authentication) when connecting to wireless networks.

## **Mobile Device Management (MDM):**

- Devices connecting to wireless networks should be enrolled in the organization's MDM solution.
- MDM policies should include device encryption, remote wipe capabilities, and application whitelisting.

## **Wireless Interference:**

- Avoid interference by ensuring proper placement and configuration of wireless access points.
- Monitor for interference and take corrective action as necessary.

## **Wireless Monitoring and Logging:**

- Implement monitoring tools to detect and respond to unauthorized access attempts or suspicious activity.
- Log wireless network activities for audit and incident response purposes.

## **Configuration Management:**

- Regularly review and update the configurations of wireless access points and controllers.
- Changes should follow a documented change management process.

## **Physical Security:**

- Physical access to wireless devices and infrastructure should be restricted to authorized personnel.
- WAPs should be installed in secure locations to prevent tampering.

## **Incident Response:**

- Establish procedures for responding to wireless security incidents, including unauthorized access or data breaches.
- Response plans should include containment, investigation, and notification steps.

## **Training and Awareness:**

- Employees and contractors should receive training on wireless security best practices.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- Awareness campaigns should highlight the risks of unsecured wireless networks and the importance of secure wireless usage.

## Related Standard, Policies and Processes

### IEEE 802.11 (Wi-Fi):

- This standard defines the specifications for wireless local area network (WLAN) communication.
- It covers protocols such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax, each with different speeds and frequency bands.

### IEEE 802.1X (Port-Based Network Access Control):

- Provides a standard for controlling access to wireless and wired networks.
- Supports authentication mechanisms like EAP (Extensible Authentication Protocol) for secure network access.

### IEEE 802.11i (WPA2 - Wi-Fi Protected Access 2):

- Specifies security protocols and encryption methods for wireless networks.
- Includes encryption protocols like AES (Advanced Encryption Standard) for secure data transmission.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## XXIX. WIRELESS COMMUNICATION STANDARD

### Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to the ASSCAT network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Committee are approved for connectivity to the ASSCAT network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by the Digital Transformation Center. Lab network devices must comply with the *Lab Security Policy*.

### Scope

All employees, contractors, consultants, temporary and other workers at ASSCAT and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of ASSCAT, must comply with this standard. This standard applies to wireless devices that make a connection to the network and all wireless infrastructure devices that provide wireless connectivity to the network.

The Infosec Committee must approve exceptions to this standard in advance.

### Policy

#### General Requirements

- All wireless infrastructure devices that connect to the ASSCAT network or provide access to ASSCAT Confidential, ASSCAT Highly Confidential, or ASSCAT Restricted information must:
- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- Lab and Isolated Wireless Device Requirements
- Lab device Service Set Identifier (SSID) must be different from ASSCAT production device SSID.
- Broadcast of lab device SSID must be disabled.



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## Wireless Device Requirements

- All wireless infrastructure devices that provide direct access to the ASSCAT network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:
- Enable WiFi Protected Access Pre-Shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a strong shared secret key on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

## REFERENCES

- ISO/IEC 27001:2013 - Information Security Management Systems - Requirements
- Information Security Policy
- Acceptable Use Policy



# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

## D. COMPLIANCE AND MONITORING

**Regular Assessments:** Compliance with the Information Security Policies shall be monitored through regular security assessments, audits, and reviews conducted by designated security personnel or external auditors.

**Incident Reporting:** Any non-compliance or security incidents related to information security shall be reported immediately to the Information Security Committee or designated security personnel for prompt investigation and remediation.

**Log and Record Maintenance:** Security logs, access control records, and audit trails shall be meticulously maintained and reviewed periodically to detect, investigate, and address unauthorized access attempts or any suspicious activities.

**Audit Frequency:** Audits and reviews will be conducted at regular intervals, with increased frequency if specific risks or incidents warrant closer scrutiny.

**Remedial Actions:** Identified issues or non-compliance shall trigger appropriate remedial actions, which may include policy updates, additional training, or disciplinary measures, to mitigate risks and enhance overall security posture.

**Continuous Improvement:** Findings from assessments, audits, and incident reports will be used to continuously improve the Information Security Policies and related controls, ensuring they remain effective against emerging threats.

**Documentation and Reporting:** All compliance activities, incidents, and remediation efforts shall be thoroughly documented and reported to relevant stakeholders, ensuring transparency and accountability.

By implementing these measures, ASSCAT aims to uphold the highest standards of information security, protecting its information assets and maintaining the integrity and trust of its operations.



## Page 87 of 87

[illegible]



## INFORMATION SECURITY POLICIES

# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Jointly prepared by:



**IRENE C. BALUIS**

Information Technology Officer I



**CLYDE ZANE MACASCAS**

Information Officer III



**SHIELA T. DELA VICTORIA**

Legal Officer IV



**ROSIELYN P. CONVERSION**

Records Officer II



**CYRUS JAY E. GALENDEZ**

Assistant Professor I



**JEANIE R. DELOS ARCOS**

Instructor I



**JANICE S. DINLAY**

VP for Student Affairs and Services



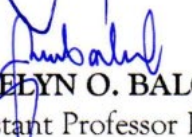
**ELMER E. ESTANDARTE**

Assistant Professor II



**LEOLYN MAE P. JUSAY**

Planning Officer III



**JOCELYN O. BALOLOT**

Assistant Professor I



**CARLO JAY P. ALBITE**

Administrative Officer V



**NANCY F. JACSALEM**

Assistant Professor II



**ESMERALDA G. CLARO**

Administrative Officer V




**VELIGEN O. BERUEDA**

Instructor



**PRIMO T. ADEM**

Supply Office III




**JENELYN S. CORCILLES**

Instructor

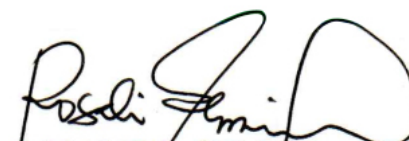


## INFORMATION SECURITY POLICIES

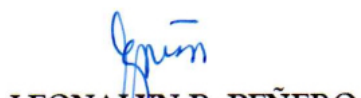
# AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY



**BERNIE S. BALIGHOT**  
Associate Professor I




**ROSALIE C. GEMINA**  
Instructor II



**LEONALYN B. PEÑERO**  
Instructor



**ANTHONETTE CAMOSA-AZARES**  
Instructor



**JAMES CLOYD M. BUSTILLO**  
Instructor I



**MICHELLE ELAPE**  
Instructor I

Approved by:



**JOY C. CAPISTRANO, Ph.D.**  
College President