UNIVERSITY OF THE BAHAMAS

Policy on Acceptable Usage

Title:	Acceptable Usage
Policy number:	POL 015
Approval(s) required	Academic Senate □ Board of Trustees ☒ Both □
Date of Senate approval if required	(dd/mm/yyyy)
Date of Board approval if required	06/12/2023
Effective date of implementation	06/12/2023
Frequency of review required	2 years
Replacing or superseding information	
Revision number	2
Responsible Office	Office of Information Technology
Accountable Officer	Chief Information Officer (CIO)
Related legislation, regulation, policy, or policies	
Appendix/Appendices	None

1. Authority

Board of Trustees.

2. Purpose

This policy establishes guidelines for utilizing the University of The Bahamas information systems. It highlights the importance of individual responsibility in maintaining a secure computing environment.

3. Scope

This policy applies to all employees, consultants, temporary, and other workers at the University of The Bahamas.

4. Definitions None

5. **Policy Statement**

5.1. The University of The Bahamas acceptable usage guidelines shall cover the following related policies and procedures:

- Computer and information system usage
- Software and data usage
- Internet and e-mail usage
- Telephone usage
- Office equipment & materials usage
- Passwords Standards

5.2 As a requirement of information systems access, and as a component of security awareness training, all information systems users, whether employees or third parties, will be required to provide signed acceptance of the acceptable usage guidelines. A copy of the signed document will be provided to the individual with the original being retained by the Human Resources unit.

5.3 Computer and Information Systems Usage

5.3.1 All systems, including computers of all kinds, are the sole property of the University of The Bahamas.

5.3.2 Access to, and use of, information systems and the components that form them will be monitored and controlled at all times by the Office of Information Technology.

5.4 Software and Data Usage

5.4.1 All software, software tools provided by the University as well as the data created and manipulated by these tools are the property of the University of The Bahamas.

5.4.2 Software is to be used for its intended purpose only. It is not to be copied, distributed, installed, or deleted without appropriate authorization. Such activities will be monitored and controlled at all times.

5.4.3 Data also is to be used for its intended purpose. It is not to be copied, distributed, edited, appended, or deleted without appropriate authorization. Such activities will be monitored and controlled at all times.

5.5. Data Security

Maintaining the confidentiality, integrity, and availability of organizational data is paramount to the security and success of the organization. To ensure that data is kept secured and handled appropriately, the guidelines below must be adhered to:

1. All organizational data is owned by the University and, as such, all users are responsible for appropriately respecting and protecting all data assets.

2. Users must keep all data secure by taking sensible precautions and following requirements defined in this policy, Data Classification Policy, and the data-handling requirements defined in the Data Classification Standard. This standard outlines the requirements for creating, using, storing, transmitting, archiving, and destroying data.

3. Data must be classified based on sensitivity, as defined in the Data Classification Policy. Data must be classified as "restricted," "confidential," "internal," or "public". Data at each classification level must be safeguarded and handled appropriately in accordance with the Data Classification Standard.

4. Users may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the University or another individual without authorized permission.

5. Users will only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.

6. Extraction, manipulation, and reporting of the University's data must be done for business purposes only.

    a) Personal use of organizational data, including derived data, in any format and at any location, is prohibited.

7. Users will follow all company-sanctioned data removal procedures to permanently erase data from devices once its use is no longer required, as defined in the Data Classification Standard. Data must be retained for the length of time defined in the Data Retention Policy.

5.6 Internet and E-mail Usage

5.6.1 Internet and e-mail usage must be restricted as both activities make use of public and unsecured networks.

5.6.2 The Internet is to be used for business purposes only and usage will be monitored and controlled at all times. When credible evidence of illegal or otherwise impermissible activities including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment (including offensive and/or insulting content), discrimination, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses), appropriate action will be taken.

5.6.3 Emails sent or received by users when conducting University business are subject to the University's Records and Retention policy and security requirements.

5.6.4 E-mail is also to be used for business purposes only and usage will be monitored and controlled at all times.

5.6.5 Should an employee or student identify hacking activities, they must report it directly to their supervisor (employee) or Office of Student Conduct and Complaints or Vice President of Student Affairs (student) and the IT Help Desk (ithelpdesk@ub.edu.bs) at the University of The Bahamas. The university bears no responsibility or liability associated with hacking, or any resulting damage.

5.6.6 Should an employee or student identify a virus or spam activity, they must report it directly to their supervisor (employee) or Office of Student Conduct and Complaints or Vice President of Student Affairs (student) and the IT Help Desk (ithelpdesk@ub.edu.bs) at the University of The Bahamas. The university bears no responsibility or liability associated with viruses, or any resulting damage.

5.6.7 Access to the University's electronic communications services is a privilege, and certain responsibilities accompany that privilege. You are expected to use the University's communication services in an ethical and responsible manner.

5.7 Telephone and Mobile Device Usage

5.7.1 The telephone system, including all telephones and fax machines, is the property of the University of The Bahamas.

5.7.2 The telephone system, is to be used for business purposes only and will be monitored and controlled at all times by the Office of Information Technology.

5.7.3 Mobile devices owned by the University of The Bahamas are to be used responsibly for business purposes.

5.8 Office Equipment and Materials Usage

All sensitive materials, such as intellectual property or information about employees, students, customers, vendors are removed from a workspace and locked away when the items are not in use or an employee leaves his/her workstation. This reduces the risk of security breaches in the workplace and is part of standard basic privacy controls.

1. Employees are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and when they expect to be gone for an extended period.

   a) Computer workstations must be locked (screen/keyboard) when workspace is unoccupied.

   b) Laptops and any other mobile devices must be reasonably secured (e.g.

   c) locked away in a drawer or cabinet) if not taken home at the end of the workday and should not be left unattended in any open area.

2. Any sensitive information (e.g. customer, employee, student, vendor data, etc.) must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

3. Passwords are not to be written down (handwritten or printed) anywhere or under any circumstances. Passwords must be secured at all times. If a password has been compromised, it should be changed immediately.

4. File cabinets containing sensitive information must be kept closed and locked when not in use or when not attended.

5. Keys/badges used for access to sensitive information or IT equipment must not be left unattended.

6. Printouts containing sensitive information should be immediately removed from the printer.

7. Before disposal, sensitive documents should be shredded.

8. Presentation surfaces (whiteboards, blackboards, projector screens, etc.) containing sensitive information should be erased.

5.9 Password Standards

Access to the University's systems and devices is controlled through individual accounts and passwords. The following requirements are in place to protect those passwords and access to sensitive data and systems:

1. Users may not share account or password information with another person. Accounts are to be used only by the assigned user of the account and only for authorized purposes. Attempting to obtain another user's account password is strictly prohibited.

2. A user must contact the IT Help Desk to obtain a password reset if they have reason to believe any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to the University's services and data.

3. Users must not use University system passwords for other services (such as personal email accounts). In the event that other services are compromised, it could leave corporate accounts compromised as well.

4. Password complexity will be enforced by IT through system-enforced policies to ensure strong passwords and proper password hygiene:

- Passwords will expire every 180 days and users will be forced to change them. Users are encouraged to reset their passwords prior to the expiry date to minimize any interruption to network access.
- A minimum lifespan of 1 day is enforced to prevent too frequent password changes.
- The previous 5 passwords cannot be reused.
- Password complexity requirements will enforce the use of uppercase, lowercase, numbers, and special characters i.e. Um5$sq%1.
- Upon 5 failed login attempts, accounts will be locked for 24 hours. Accounts can be unlocked by contacting IT Help Desk or waiting for the 24 hours to elapse.

5.10 Non-Compliance

Violation of any of the restrictions of these policies or procedures will be considered a security breach and will be investigated per the University's established procedures and depending on the nature of the violation, various sanctions will be taken:

1. Oral and/or written warning
2. Probation, suspension, termination or expulsion
3. Legal action per applicable laws and contractual agreements

6. **Procedures:** None

Appendices: None