ACCESS CONTROL STANDARD

1. Purpose

The purpose of this standard is to protect Wayland Baptist University's information assets by establishing controls for granting and removing access.

2. Scope

This Standard is applicable to the University's employees, contractors, and third-party service providers.

Information Security Standards support Information Security Policy, and are not intended to supersede or conflict with said policy.

3. Definitions

3.1. ***Information Systems:*** Collections of hardware, software, and services for collecting, processing, storing, and delivering information.

4. Roles and Responsibilities

4.1. ***Information Owners*** are responsible for maintaining processes and procedures to control and prevent unauthorized access to information they have been designated ownership.

4.2. ***Human Resources*** is responsible for maintaining processes to notify Information Custodians when user's access should be removed due to changes in employment or contractual relationship.

4.3. ***Managers and Supervisors*** are responsible for approving access requests of their direct reports, and notifying Human Resources of changes in employ

4.4. ***Information Custodians*** are responsible for maintaining processes and procedures to manage access to Information Assets within the span of technical and organizational control.

5. General Requirements

5.1. Access to Information Assets shall follow the principle of Least Privilege (Information Security Policy 5.1) according to provisioning procedures authorized by Information Owners.

5.2. Access provisioning procedures shall be designed and managed according to the principle of Separation of Duties (Information Security Policy 5.2), requiring more than one individual to request, approve, provision, modify, or revoke access. **PLEASE NOTE:** Accounts may be temporarily suspended or passwords changed pursuant to the Security Incident Management Standard.

5.3. User Accounts shall be unique and used solely by the individual to which the account is assigned.

5.4. User Accounts shall be created according to a naming convention that allows consistent association with the individual to which it is assigned.

5.5. Shared or anonymous accounts shall be limited and controlled according to procedures reviewed by the Department of Information Technology.

5.6. Access to WBU systems from external networks shall be granted through Multi F.anted thr112 0 612 92 reW*nBT

7.3. Default account credentials are not permitted on Information Assets. All default accounts shall have passwords changed immediately following the installation of supporting systems and software. Default accounts shall be removed or disabled where possible. For systems where disabling or removing default accounts is not possible, Information Custodians are responsible for monitoring and documenting use of default accounts.

8. Compliance and Enforcement

Information Custodians are responsible for monitoring compliance with this policy and reporting instances of non-compliance to President's Cabinet or their designee.

9. Exceptions

Exceptions to this standard shall be reviewed by the Department of Information Technology and designated ad hoc committees from President's Cabinet as needed. No exceptions shall be made without prior approval of Cabinet.

10. Effective Dates

This standard is in effect with Information Security Policy, upon adoption and renews with the Information Security Policy, originally approved by Cabinet March of 2022.