CATS – TWO-FACTOR AUTHENTICATION BY-PASS POLICY AND PROCEDURE

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.0	7-24-2017	Michael Natale	Initial Publication - DRAFT
1.1	9-21-2021	John Remley	Fixed links and made official
1.1	4-20-2022	Mike Natale	Annual Review
1.1	2/21/2024	Mike Natale	Annual Review

	Wright State University Information Security	

Controls	
Policy Title:	Two-Factor Authentication By-pass Policy and Procedure
Category:	Information Technology
Audience:	WSU Faculty and Staff
Reason for Revision:	*N/A*
Created / Modified Date:	9-21-2021
Next Review Date:	9-21-2022
Location:	http://www.wright.edu

Responsible Parties	
Author	Michael Natale
Technical Reviewer/Mgr	Michael Natale
Security Reviewer	John Remley

Background

Two Factor Authentication (2FA) provides a second layer of protection to a user's digital identity and to WSU's data, systems, and services.

Users are strongly encouraged to enroll more than one device but this will not be required. Whether it's an instance of a single enrolled device not being available (broken or lost) or a malfunctioning primary device being the only one available (mobile device isn't working while away from a back-up landline), users will occasionally find themselves unable to gain access to WSU's websites and services and will consequently request a temporary solution. A bypass codes provides that temporary solution, granting a user access to 2FA-protected sites when an enrolled 2FA device is temporarily unavailable.

Scope

This Policy applies to all faculty, staff, students, and any third parties designated as agents authorized to handle institutional data and/or access University computing systems.

Policy

The Office of the CIO and the Information Security Department authorizes the use of bypass codes based on the following criteria:

Conditions to Issue Bypass Codes

- Requester must be identity proofed (following standard CaTS Service Desk process).
- No other enrolled device options are available.
- No secondary device is available for enrollment.
- No temporary device is available for enrollment.
- Immediate access to WSU's systems is needed.

Who Will Issue Bypass Codes

- The bypass codes will be issued by appropriate CaTS staff members
- Select CaTS Service Desk personnel.
- Operators
- Duo Admins and designated Client Services team members.

Bypass Code Details

The number of uses for the bypass code issued to an individual user and the expiration time for the code will be determined based on a conversation between the support personnel and the individual requesting the bypass code (an expiration of no more than 12 hours may be granted). The goal is to determine the fewest number of uses with the shortest expiration time that will satisfy the needs of the user until a currently enrolled device becomes available or a new permanent or temporary device becomes available to enroll with the service. If other options are needed escalate to Duo Admins.

Based on the above conversation:

- Multiple-use codes (one code that can be used multiple times)
  - The user can use this code unlimited times within 12 hours (set to a maximum of 720 minutes) to get them through a workday.
- Whether used or not, set all Codes to expire in no more than 12 hours (720 minutes).

  Note: The expiration time of a bypass code is an indication of when the code itself will expire if it is not used; it is not the expiration time for the active session created by an authentication using that code. For instance, a bypass code that is set to expire in 12 hours could be used to authenticate into a 2FA-protected service 11 hours and 59 minutes after being issued, and the authenticated session would then last for an extended period. For instance, a Wings session might last 8 hours unless the user logs out.

Tracking of Bypass Codes

Enter the use of all bypass codes into ServiceNow. ServiceNow entries should include the reason for the request. CaTS will conduct periodic reviews of bypass code use to ensure proper handling.

Associated WSU Policies

Guidelines for Protected Information – refer to this document for guidelines on computing habits & protected information.

Wright State University IT Security Policy – refer to this document general IT Security practices currently in place.

Wright State University Information Security Framework – This policy outlines the information security program within Wright State University.