Two-Factor Authentication Policy

ROWAN UNIVERSITY POLICY

Title: Two-Factor Authentication Policy
Subject: Information Resources and Technology
Policy No: IRT:2018:04
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Vice President for Information Resources and Technology and Chief Technology Officer
Date Adopted: 07/02/2018
Last Revision: 01/11/2022
Last Review: 01/11/2022

I. PURPOSE

Two-factor authentication adds a second layer of security to Rowan NetID accounts. This second form of authentication helps to prevent unauthorized access to an account even if the password is compromised. Rowan University currently uses a product called Duo for two-factor authentication.

Duo can provide a second form of authentication via a mobile device app, phone, or hardware token. The mobile device app is recommended. Rowan users must use at least one (1) but are encouraged to have at least two (2) registered methods of two-factor authentication in Duo so that they can always log in to a Rowan service even if one method is temporarily unavailable.

Using Duo for two-factor authentication is mandatory for all Rowan services protected by Duo.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Chief Information Security Officer shall ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all members of the Rowan community who use Rowan services that are protected by Duo two-factor authentication.

IV. DEFINITIONS

1. **Two-factor authentication** adds a second layer of security to a Rowan NetID Account. Some services and websites refer to this second layer of security as two-factor authentication, 2FA, two-step authentication, two-step verification, or login verification. This second form of authentication helps to prevent unauthorized users from accessing an account, even if the password is compromised.
2. The **Duo Mobile app** is available for phones and cellular capable devices, both Apple and Android. It is available for free from the Apple App Store and Google Play Store. It allows the user to say “Yes” or “No” to any attempted login to their account for Duo protected services and thereby provides a second factor of authorization for these services.

3. A **phone** is a device capable of receiving phone calls or text messages. It allows the Duo system to contact a user by voice or text message in order to ask them to agree to any attempted login and thereby provides a second factor of authorization to services protected by two-factor authentication.
4. A **hardware token** is a small device that can generate a passcode which can be used as a second factor of authorization to services protected by two-factor authentication.

Refer to the Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

V. POLICY

1. Rowan requires all individuals, including employees, students, affiliates, retirees and alumni to use either the Duo Mobile app or a phone as a method of two-factor authentication. This can be supplemented by the use of a hardware token where necessary, see below.
2. Rowan recommends that all individuals enroll a second device for two-factor authentication to use if their required method is unavailable. This second option may be the other of the two options listed in V. 1, or may be a hardware token.
3. Hardware tokens may be obtained by all employees, employee affiliates with access to HIPAA classified data, students, and student affiliates. Hardware tokens are not available for retirees, alumni or affiliate employees who do not have access to systems hosting HIPAA data. The Information Security Office may approve the distribution of hardware tokens to any individual as a documented exception.

	Employee	Student	Medical Student	Alumnus	Retiree	Employee Affiliates	Medical Affiliates	Student Affiliates
Mobile - App	Y	Y	Y	Y	Y	Y	Y	Y
Mobile - SMS	Y	Y	Y	Y	Y	Y	Y	Y
Mobile - Voice	Y	Y	Y	Y	Y	Y	Y	Y
Landline - Voice (External DID)*	Y	Y	Y	Y	Y	Y	Y	Y
Landline - Voice (Rowan Internal non-DID)*	Y	Y	Y	Y	Y	Y	Y	Y
Hardware Token	Y	Y	Y	N	N	N	Y	Y

* DID aka Direct Inward Dialing refers to phone numbers that may be dialed directly from outside of the University. Phone extensions that are internal to the University are referred to as non-DID numbers. Non-DID numbers at organizations outside of Rowan University are not supported by Duo.

4. Replacement hardware tokens may be requested once per year in cases of damage or loss.
5. Hardware Token Recycling or Disposal
    a. Tokens may be returned to any designated IRT office for recycling or disposal.

VI. POLICY COMPLIANCE

Violations of this policy may subject the violator to the removal of system access or disciplinary actions, up to or including termination of employment or dismissal from a school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization per the Acceptable Use Policy.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer