LIBRARY, ICT SERVICES & ARCHIVE

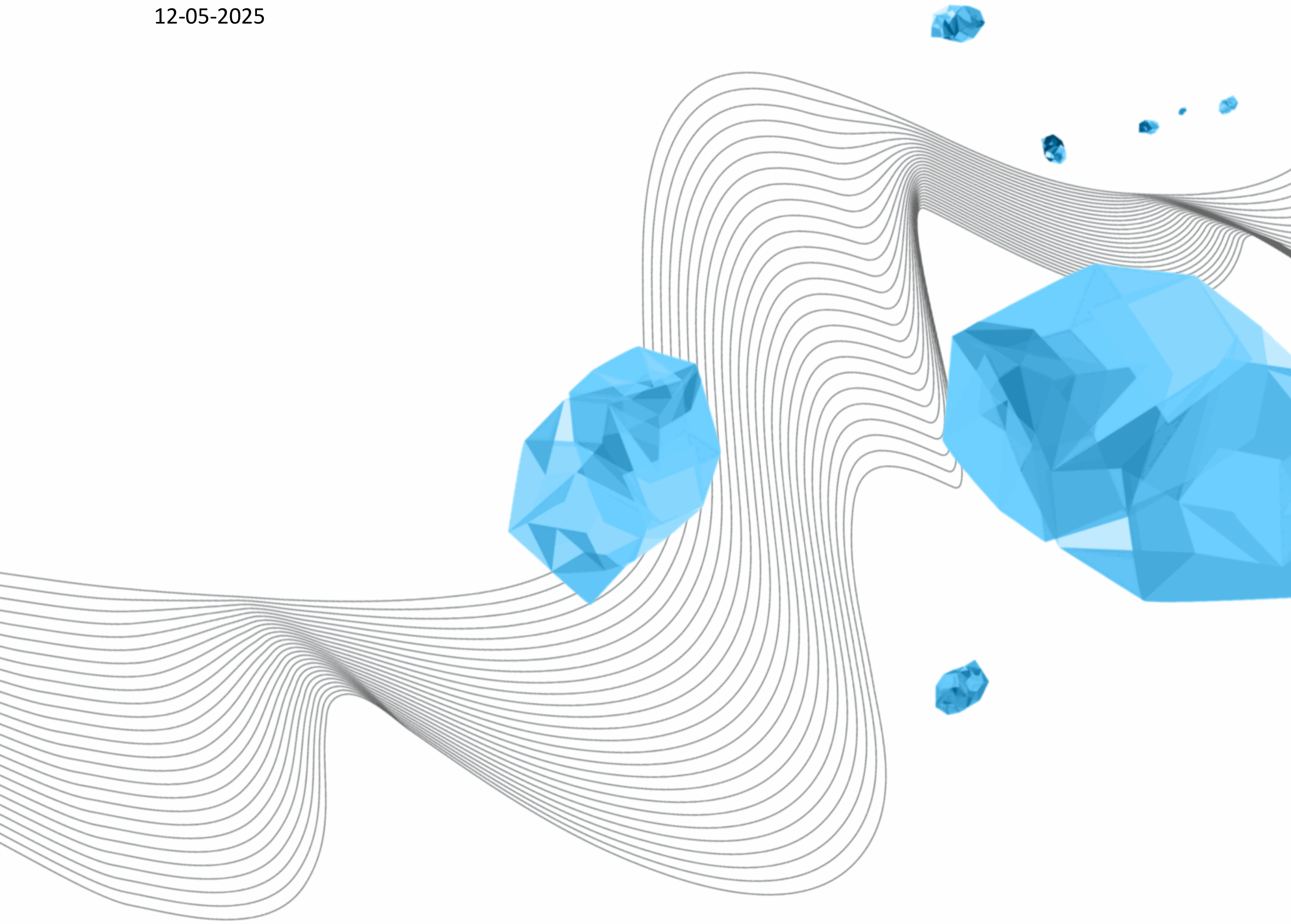
GUIDELINES ON IDENTITY & ACCESS MANAGEMENT

AUTHENTICATION METHODS

Peter Peters

Versie 1.4

12-05-2025



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Guidelines on Identity & Access Management

SUBJECT
Authentication Methods

VERSION (STATUS)
1.4

DATE
12-05-2025

AUTHOR(S)
Peter Peters

COPYRIGHT

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	REMARKS
1.0	25-10-2022	Peter Peters	Approved by LISA-MT
1.1	28-2-2023	Peter Peters	Rewrote appendix on password managers. Rewrote chapter 5 to include Number Matching.
1.2	2-10-2023	Peter Peters	Removed the option for SMS authentication, as Microsoft has phased this out.
1.3	13-6-2024	Peter Peters	Removed references to TAP. Updated Chapter 6 to latest information regarding passwordless authentication
1.4	12-5-2025	Peter Peters	Changed reference to password reset procedure

DISTRIBUTION LIST

VERSION	DATE	DISTRIBUTED TO
1.0	25-10-2022	Published on Cyber Safety website
1.1	28-2-2023	Published on Cyber Safety website
1.2	4-10-2023	Published on Cyber Safety website
1.3		Published on Cyber Safety website
1.4	20-5-2025	Published on Cyber Safety website

CONTENT

1 INTRODUCTION

This document replaces the old password policy dating to 15 June 2015.

This document is a document with guidelines and not a policy. For the policy on Identity and Access Management, we refer to the Policy on Information Security.[1] By making this a document of guidelines, it will not have to go through the standard process for establishing policies at the University. It will make it easier to change the guidelines when changes in technology occur.

As the basis of this document, we will use best practices and guidelines from security experts and national and international (security) agencies. Among the most important are the *Nationaal Cyber Security Centrum (NCSC)*[2] and the *National Institute of Standards and Technology (NIST)*[3] of the U.S. Department of Commerce, especially SP 800-63B[4], **requirements to credential service providers for remote user authentication**.

Readers can read more about the information security organisation and its roles in the Policy on Information Security. [5]

Identity and Access Management (IAM) consists of several separate, sometimes overlapping, sometimes closely coupled parts.

1. Identification, including the provisioning of identities
2. Authentication
3. (Role-Based) Access Control (RBAC)

The scope of this document is authentication. Separate guidelines will be provided on the kind of identities and their life cycle. Lastly, guidelines will be compiled on how to perform Role-Based Access Control at the University.

2 AUTHENTICATION

The standard authentication method at the university is **multi-factor authentication (MFA)**[6]**.** The factors used at the University are a password and a token.

Users SHALL NEVER share Passwords, PINs, or devices as part of a user's authentication process.

MFA is mandatory.

3 PASSWORDS

Any password used SHALL be a 'strong' password. Strong passwords are not easily guessed by people having information about you, like your birth date, the names of your pets, the brand of your car, the names of family members, and more. Also, using only one or two dictionary words is

[1] https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/policy-on-information-security.pdf
[2] https://ncsc.nl/
[3] https://nist.gov/
[4] https://pages.nist.gov/800-63-4/sp800-63b.html
[5] Chapter 4.3 and chapter 5.
[6] When using the university's Single Sign-On system Multi-Factor Authentication is enforced.

discouraged, especially in the users' language. A weak password does not become a strong password by merely replacing letters with other characters that look alike, e.g., replacing a lowercase L with a 1 or an S with a $ sign.

A strong password is a string of random characters, three or more random (dictionary) words, or a passphrase.

A *random password* consists of an actual arbitrary string of characters from all character sets allowed. A random password is difficult to remember. Therefore, LISA advises using a Password Manager (See appendix).

Using *random words* (at least 3), perhaps even from different languages, will make a password hard to guess and therefore "strong". It will make it easier for you to remember than entirely random passwords.[7]

The third way to make a strong password is to use a *passphrase*. A passphrase is an easy-to-remember sentence that makes sense to you (and only you) and is usually very easy to remember.

"Iate2greenpotatos,nice!" is an excellent example of a passphrase.[8]

A password SHOULD NOT be written down or stored in an insecure way.[9]

A user SHALL NOT use passwords used for any account at the University for any other account. This guideline is relevant for both accounts used outside the University, e.g., social media, and all accounts at the University. A password for the standard UT account SHOULD NOT be used for accounts with special privileges, and it SHOULD NOT be used in applications that do not use the University's Single Sign-On system.

4 CHANGING PASSWORDS

Passwords don't need to be changed on a regular base.

The university uses Microsoft's Single Sign-on Service. Users can use Microsoft’s portal[10] if they want or need to change their password.

A user SHALL change their password when they expect it to be compromised.
If you suspect your password is compromised, contact the Computer Emergency Response Team of the University of Twente, CERT-UT.[11] Even if you are in doubt, contact CERT-UT.

CERT-UT can deactivate a user's account or reset its password. This should only be done when there is reasonable suspicion that the account has been compromised. After the account is enabled again, **the user SHALL change their password within 24 hours**.

[7] https://xkcd.com/936/

[8] Do not use this passphrase or something like it with only slight modifications! This document is published publicly, so this password can end up in a list criminals use to test. See Chapter 4 for guidelines on (re)using passwords.

[9] Using a Password Manager (see appendix) is considered securely storing your password. Any other method is considered insecure.

[10] https://myaccount.microsoft.com/

[11] cert@utwente.nl or (+31 53 489)1313.

A user SHALL not reuse any of their passwords.[12] This includes passwords used for their account at the University or any other password used currently or in the past for accounts outside the University. A password more than 50% identical to another password is considered a reuse of that password.

If users have lost or forgotten their password, they can reset it using the Microsoft portal[13] or contact Servicedesk ICT[14].

5 MULTI-FACTOR AUTHENTICATION

In the case of multi-factor authentication, a user has to provide more than one authentication factor. Some factors are not as secure as others but increase total security when used together.

Under normal circumstances, the University recognises three factors:

1. Something you know, like a password or PIN;
2. Something you have, like a phone or hardware token;
3. Something you are, like a fingerprint or facial characteristics.

The default multi-factor authentication settings at the University will require your password as the first factor and your phone as the second.

Using your phone as the second factor requires an authentication app. Any application supporting the Time-based One Time Password[15] (TOTP) standard can be used. In that case, the application will provide you with a 6-digit number. That number changes every couple of seconds.

The Microsoft authenticator allows the university to use some extra features.

- The app can show information about the application requesting authentication.
  The university uses this feature.
- The app can show information about the user's location.
  The university does NOT use this feature.
- The authentication page from Microsoft can show a 2-digit number, which the user has to copy to the app.
  The university uses this feature.

In some cases, and only after permission from the CISO, the second factor can be "someplace you are, like on a specific computer." This is considered an exception to the standard MFA guidelines, though, and **permission SHALL only be granted for a limited time**.

The university will not offer authentication methods that are considered insecure, like text messages (SMS).[16]

[12] If possible, the system used to change passwords SHOULD check the history of used passwords.

[13] https://passwordreset.microsoftonline.com/

[14] Servicedesk-ict@utwente.nl or (+31 53 489)5577.

[15] https://en.wikipedia.org/wiki/Time-based_one-time_password

[16] Criminals use SIM swapping, where they abuse the telecom's user-friendliness to copy your phone number to their phone. The second-factor code is sent to their phone when they access your account. See also https://en.wikipedia.org/wiki/SIM_swap_scam

6 PASSWORDLESS AUTHENTICATION

Passwordless authentication is an authentication method in which a user can log into a computer system without providing (and thus having to remember) a password. Passwordless authentication can be implemented in several ways. Currently, the University supports the following methods:

1. Passkeys in Microsoft and other authentication apps.
2. Security keys, like Yubikey, that support the FIDO2 standard[17].
3. Windows Hello, on Windows 11.
4. PIN, in a few limited situations.

With methods 1 and 3 the user has to verify the authentication on the device by providing a PIN or using biometric means, like a fingerprint. Method 4 is only used to log into managed Windows workstations.

Method 2 is considered phishing-resistant MFA and the only method allowed for privileged accounts, as referred to in chapter 7.

7 PHISHING-RESISTANT AUTHENTICATION

Phishing attacks are attempts by fraudulent parties to fool an unwary user into presenting an authenticator to an impostor. The term phishing is widely used to describe a variety of similar attacks. In this document, phishing resistance is the ability of the authentication protocol to prevent the disclosure of authentication secrets and valid authenticator outputs to an impostor without relying on the user's vigilance. How the user is directed to the impostor is not relevant.

The University will define in which cases phishing-resistant authentication is mandatory.

The phishing-resistant authentication currently supported is based on W3C Webauth[18], which is used by authenticators that implement the FIDO2[19] specifications.

8 EXCEPTIONS

8.1 PRIVILEGED ACCOUNTS

Holders of privileged accounts SHALL receive special instructions about changing their passwords.

A password for privileged accounts SHALL be at least 20 random characters or a passphrase of equal length.

Passwords with privileged identities SHALL be changed every six (6) months.

The use of phishing-resistant authentication is mandatory for these accounts.

[17] https://en.wikipedia.org/wiki/FIDO2_Project

[18] https://www.w3.org/TR/2021/REC-webauthn-2-20210408/

[19] https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html

8.2 FUNCTIONAL ACCOUNTS

Suppose the composition of a group changes; the team lead SHALL have all passwords shared with that group changed. Consider, for example, a functional account used by several people.[20]

If the team uses a password manager to restrict access to passwords AND offers audit logging to check which users access what passwords, it is allowed to only change passwords the leaving team member had access to.

9 PASSWORD MANAGERS

The University promotes the use of a Password Manager.

A Password Manager is either a stand-alone application, part of another application like a browser, or an integral part of the Operating System. In most cases, the solution offered by the Operating System or browser is adequate for storing personal passwords.

Stand-alone Password Managers offer extra features regarding the data that can be stored[21] and ways to synchronise between different devices and different Operating Systems. It can also help store shared passwords.

If you are using a Password Manager, you must have a "very strong" master password. This password gives access to all your passwords and, therefore, to all accounts. It is best to use a passphrase here.

Users SHOULD use a Password Manager.

[20] Incidentally, accounts used by several people are only allowed with a high exception. To create these accounts, prior permission from the CISO is required.

[21] For instance, information about your banking accounts. It can often also store ID, like your passport, including a picture of your passport.