Password Policy of the Technical University of Darmstadt

–Translation help, the German version is binding–
IT Security at TU Darmstadt
Published: December 9, 2021

TECHNISCHE UNIVERSITÄT DARMSTADT

IT-Sicherhe!t
Informationssicherheit | TU Darmstadt

Identifiers

Title (Document abbreviation):	Password Policy of the Technical University of Darmstadt (PW-RL)
Creator:	Johannes Braun / Review: Jochen Becker
Roll of the creator:	Chief Information Security Officer / Head of TUDa-CERT
Version number:	v02
Last Revision:	December 10, 2021
Next planned Review:	November 2022
Approved on / by:	November 26, 2021 / Herbert De Gersem, Vice President of Scientific Infrastructure and Digitization
In effect since:	since publication, Transition period until April 4, 2022
Classification:	public
Eligible Rolls (distribution circle):	all members of TU Darmstadt
Change log:	v01 $\rightarrow$ v02: Expansion of allowed special characters

Abstract

The goal of this policy it to ensure an adequate level of security, for use in a username/password-procedure. The necessary fundamental regulations and instructions for action are listed below. Relevant IT protection modules (IT-Grundschutz Bausteine) are listed in the bibliography at the end of this document.

Contents

1 Area of application

This policy applies to the whole IT infrastructure operated by the Technical University of (TU) Darmstadt, consiting of data processing systems, communication systems and further auxiliary facilities. This includes commissions of IT subcontractors.

This policy applies to all users and operators of IT infrastructure at TU Darmstadt.

2 Password requirements

The guide below determines the requirements for passwords.

2.1 General password requirements

- The password must have a length between 12 and 30 characters.
- Allowed characters are:
  - Upper case letters: A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
  - Lower case letters: a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z
  - Numbers: 0,1,2,3,4,5,6,7,8,9
  - Special characters: ! " $ % & ' ( ) * + , - . / ; < = > ? { | } ~] @
- Passwords must not contain personal data, names, or IDs of users.
- Passwords must not be words contained in a dictionary, regardless of the language.

2.2 Password requirements for administrative accounts as well as Proxy and Gateway accounts

- The password must have a length of at least 20 characters.
- The password must randomly generated using a random password generator (e.g. “pwgen 20” or KeePass).
- For allowed characters see 2.1.

3 Rights and obligations when handling passwords

In the following, the rights and obligations of users in their role as system users or system operators are defined..

3.1 Initial choice of passwords

- For each service a new password must be used.[1]
- Passwords set by administrators or set by a computer system must be changed during the first access.
- As far as possible, passwords should be generated randomly. The use of password generators combined with a password manager (e.g., KeePass) is recommended.
- In order to obtain retainable passwords, password sentences can be used.[2]
- Use as many character sets from 2.1 as possible.

3.2 Usage of passwords

- While entering a password, ensure no one is observing the input.
- Passwords within the area of application of this policy must not be entered on unsecured (foreign) systems.
- Personal passwords must not be shared with third parties.
- Passwords of system administrators must only be known to personnel who need them to carry out their assigned tasks. If a person leaves the group of authorized people (e.g., by exiting TU Darmstadt), the passwords in question must be changed.
- A password must be changed if it became known to an unauthorized person or if there is reasonable suspicion that it has been leaked.

3.3 Storage of passwords

- Unencrypted storage of passwords on IT systems is not permitted.
- Encrypted storage in a password manager (e.g., KeePass) is permitted.
- Writing passwords on paper should be avoided. Should it be necessary to write a password on paper, it must be kept in a secure, access protected location.
- For emergencies, a written password can be deposited in a safe/vault.

[1] The TUDa SSO (Single Sign-On) is to be considered as a single service.

[2] Think of a sentence and pick the first letter of each word (or 2nd or 3rd etc.) Transform some letters to numbers or special characters. An example (please do not use it as password right away): “In the morning I get up and brush my teeth for three minutes.“ This would give us: ItmIguabmtftm. Exchange every I by a 1, replace the ”and” by ”&” and capitalize nouns. Now we have ”1tM1gu&bmTftM”.

4 Rights and obligations of system operators

Operators of authorization systems must follow some fundamental regulations and can enact further security mechanisms. System operators can enact further requirements for passwords that exceed this policy. These requirements must at least match the security level of this policy. As technology permits, compliance of system users with the requirements of this policy should be checked on the system side. Here, at least the password length must be checked.

4.1 Storage and access protection

- Access to password databases must be protected by cryptographic means according to the state of the art.
- Over insecure networks, passwords must only be transmitted in encrypted form.

4.2 Intruder lockout and attack protection

- A procedure to reset passwords must be defined.
- An automatic account lock must come into effect after 5 incorrect password entries.
- An automatic account lock must lock the account for a minimum of 5 minutes (blocking period).
- The automatically enacted account lock must not be reversed before the end of the blocking period. This can be automated.

4.3 Quality assurance of passwords

- During the procedure of setting passwords, system operators can take technical measures to check conformity with the current policy. Among other things, a plausibility check can be performed to prevent trivial or easily guessable passwords.
- System operators can use automated programs to check the passwords of their complete user base. Such a program must be designed such that the the actual user passwords are not revealed to the system operator. Accounts associated with invalid or insecure passwords can be locked immediately. The respective users must be prompted to change their passwords.

References

[1] BSI. “ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B)”. In: *IT-Grundschutz-Kompendium*. Vol. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[2] BSI. “ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb] (B)”. In: *IT-Grundschutz-Kompendium*. Vol. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[3] BSI. “ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B)”. In: *IT-Grundschutz-Kompendium*. Vol. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[4] BSI. “ORP.4.A11 Zurücksetzen von Passwörtern [IT-Betrieb] (S)”. In: *IT-Grundschutz-Kompendium*. Vol. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[5] BSI. “ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen [IT-Betrieb] (S)”. In: *IT-Grundschutz-Kompendium*. Vol. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.