UHH Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Password guidelines

Version 1.0

Section 1 Scope

(1) These guidelines regulate the composition and management of passwords used to authenticate authorized users. Separate guidelines apply for administrative passwords.

(2) These guidelines apply for all IT and telecommunication systems whose resources and data must be protected using passwords to the extent technically possible to prevent unauthorized access, misuse, or modification.

Section 2 User obligations

(1) Passwords must be kept secret and entered without being revealed. In particular, they may not be stored on function keys or saved on computers in an unencrypted format.

(2) The password length depends on the data and resources requiring protection and must comprise at least 8 characters. A password containing at least 10 characters must be used to protect user accounts with special rights and tasks (e.g., security functions or applications containing sensitive data).

(3) Passwords must be as complex as technically possible (i.e., comprise upper and lower case letters, numbers, and special characters). This is the most important protection against systematic spying. Also see Appendix 1 to these guidelines.

(4) Passwords that are easy to guess may not be used. In particular, avoid:

1. repeating characters;
2. numbers/data that relate to your personal life;
3. character combinations that differ only slightly from previous passwords;
4. simple combinations of numbers and letters;
5. characters that are on adjacent keys on the keyboard;
6. character combinations that correspond to search terms in dictionaries and encyclopedias (trivial passwords).

(5) Passwords must be changed after a period of time appropriate to the level of protection required for the data and resources. In the absence of further provisions, this must be after 180 days at the latest.

(6) As a rule, passwords may not be changed more than once a day. However, they must be changed immediately should it be suspected that they have become known to a third party.

(7) Temporary passwords must be replaced with personal passwords without delay.

(8) A password-protected screen saver or screen lock must be set for end devices to prevent access to the logged-on end device after a period of time that depends on the level of protection required for the data and resources. The regulations in these guidelines apply accordingly to the unlocking of end devices using a password.

Section 3 Obligations of the system administrators and program developers

(1) Password files must be protected against unauthorized access.

(2) Passwords assigned automatically during software installation must be replaced with a new one without delay.

(3) The length of and validity period for passwords that are not entered as part of the login procedure (application-related passwords) are subject to the protection requirements of the application and data to be processed. Deviations from the requirements stipulated in Section 2 paragraphs 3–5 are possible should additional protection not be necessary.

(4) Software must be designed or configured so that users can assign passwords only with a minimum length of 8 characters. Specifications for application-related passwords must take the protection requirements of the respective application into account.

(5) Failed password entry attempts must be logged. The logs must be evaluated regularly to detect any attacks and/or misuse.

(6) Wherever possible, software measures must be implemented to ensure that:

1. only passwords comprising the greatest possible mix of upper and lower case letters, numbers, and special characters can be set;
2. a change of password is required after the period specified and at the latest after 180 days;
3. new usernames that are not activated within 90 days are blocked;
4. passwords are not displayed on the screen;
5. passwords are stored in a one-way encrypted format, in line with the current state of technology;
6. usernames are blocked after the password has been entered incorrectly 5 times;
7. passwords in networks are transmitted in an encrypted format;
8. passwords that are easy to guess cannot be assigned.

(7) If it is not possible or sensible to block a username after the password has been entered incorrectly 5 times, other equivalent measures must be taken (e.g., a time delay before renewed password entry attempts).

(8) When selecting IT systems, the availability of appropriate mechanisms must be taken into account. If these are not available on the operating system or application level, suitable additional software must be used.

Section 4 Procedure for resetting automated passwords

(1) Insofar as it is technically and organizationally possible, an automated procedure is used for resetting passwords. Users of the automated procedure must assign a master password in advance that meets the specifications stipulated in Section 2 paragraphs 3–5, which can be used for subsequent user authentication and must therefore also be kept secret. If technically feasible, a TAN procedure using a TAN sent via SMS can also be used.

(2) Should a user wish to use an automated procedure to access Universität Hamburg procedures or a workstation's user interface, they can reset their password for themselves by following these steps:

1. Enter the master password.
2. If the correct password is entered, the user will be prompted to enter a new password for the username (also see Section 2 paragraph 7).

(3) The data protection officer at Universität Hamburg must be informed before an automated procedure is introduced.

Section 5 Obligations of the password managers

(1) If an automated password reset is unsuccessful or not possible, an authorized individual must reset the password. At the request of an authorized individual, the office responsible for password management unblocks the username or neutralizes the user password once it has verified the identity of the authorized individual. If a username has been blocked by someone responsible for authorizing users, the password manager may unblock the username only at their request.

(2) The unblocking and neutralization of passwords must be documented in an auditable manner so that it is possible to trace who requested this and how their authorization and identity were verified.

(3) The temporary password assigned by the password manager (e.g., to unlock or neutralize a password) must be communicated in such a way that unauthorized access is prevented. At the same time, the recipient of the temporary password must be prompted to change the temporary password without delay.

(4) The username owner must be informed of a password neutralization if s/he did not initiate it and must at the same time be prompted to change the neutralized password without delay.

(5) Usernames that are no longer required or have not been used for longer periods of time must be blocked, unless it is necessary for the functionality of operations in general for a username not to be blocked. This also applies to IDs for (remote) maintenance.

Section 6 Organizational measures

(1) Insofar as data and resources require such protection, passwords must be an appropriate length (i.e., comprise at least 10 characters) and valid for less than 180 days. Particularly the potential damage that would arise if an unauthorized individual were to use the password over a longer period of time and the risk that an unauthorized individual could use the password for a longer period of time after gaining knowledge of it must be taken into account when determining an appropriate validity period.

(2) Appropriate measures must be taken to ensure that these guidelines are adhered to.

(3) Employees must be informed of the contents of these guidelines accordingly.

Section 7 Other measures

(1) Usernames must be assigned on an individual basis.

(2) If methods of authentication other than passwords are used (e.g., a magnetic card, chip card, or token), they must be managed in such a way that any unauthorized use is prevented. The responsible bodies must issue special regulations in this regard as necessary.

Section 8 Exceptions

The responsible office may grant exceptions to these guidelines if the principles of data protection and data security are adhered to and there is no risk to the IT infrastructure. Sections 8 and 9 of the Hamburg Data Protection Act must be observed. In particular, the process description and risk analysis must be adapted and the data protection officer at Universität Hamburg involved.

Section 9 Effective date

These guidelines become effective on 26 May 2016 through the resolution of the Chief Information Officer Board.