Leibniz-Rechenzentrum

POLICY FOR THE SELECTION AND USE OF PASSWORDS AND PASSPHRASES

20. Mai 2020

1 OVERVIEW

The LRZ uses authentication procedures to ensure secure access to its systems and services. In most cases these are password-based or related mechanisms where users will

- either directly enter the password assigned to their LRZ account in the LRZ ID portal,
- or protect other information required for authentication – for example the private key of an SSH key pair – with a password or passphrase.

  This policy defines the obligations of all users of LRZ services and systems in the selection and use of passwords and passphrases for LRZ accounts allocated by Master User; different policies apply to LRZ accounts allocated by CampusLMU, TUMonline or Grid Projects.

2 TERMINOLOGY: PASSWORDS / PASSPHRASES

In the LRZ ID portal a password can be assigned to each account issued by the LRZ user administration. Entering a login-name and the associated password to access an account is a well-established authentication procedure and is used for many LRZ services and systems.

The term passphrase derives from the context of authentication procedures based on public/private keys, which may be used for selected LRZ services and systems, e. g. SSH key pairs and (Grid) user certificates. Here, authentication is achieved by a secret private key, generally stored as a file in the user's home directory. This file must be encrypted to protect it from unauthorized access. This is usually effected by the respective application, e. g. the SSH client or Grid middleware tool, which will prompt the user to enter a passphrase. Instead of a single password a series of words or a phrase with properties similar to a password must be entered.

In the following text usually the term password will be used; however, the rules apply with the necessary modifications to passphrases as well.

3 SCOPE

This policy applies to all LRZ users whose LRZ account is created by Master User. It covers

- all IT services and systems which are provided, operated or managed by the LRZ,
- all accounts created in these IT services and systems, regardless of whether they are central or local accounts,

- all authentication procedures based on or otherwise relying on passwords. This specifically includes the use of passphrases to protect the private keys of SSH key pairs and (Grid) user certificates.

Individual service and system providers may define and implement additional stricter rules if necessary.

LRZ employees are covered by a separate policy which enforces stricter rules than those established here.

4 GOALS

The most frequent cause of security incidents at the LRZ are compromised accounts, where attackers acquire knowledge of the corresponding password. This policy seeks to ensure that login-name/password and similar authentication methods are employed with the required level of security.

To this end the policy defines the user obligations for all services provided on LRZ servers. It is designed to help users avoid mistakes in the use of logins and password-based authentication procedures and at the same time prevent successful attacks by ensuring that all users employ high-quality passwords.

5 RULES FOR THE SELECTION AND USE OF PASSWORDS AND PASSPHRASES

§1) Password quality: to make it difficult to guess passwords by, for example, dictionary attacks or the systematic trial of all possible character combinations, the following rules for the choice of passwords apply:

1. The password must consist of at least eight characters. Privileged accounts (e.g. system administration) must be secured by passwords of up to 20 characters.
2. The password must be as complex as possible, with capital and lower-case letters, numbers and special characters. It must contain at least two letters and at least one numeral or one special character.
3. When a password is changed, the new password must differ from the old one in at least three places. It may not include the login-name of the account, not even in permuted form.
4. The password must not be easy to guess. In particular, the following should be avoided
    a. repeated characters,
    b. numbers and data based on the user's personal information,
    c. simple letter and number combinations,
    d. sequences of characters like 1qay2wsx which represent neighboring keys,
    e. character combinations representing search terms in dictionaries or encyclopedias.
5. Passwords for LRZ accounts must differ from passwords for services provided outside the Munich Science Network.

§2) Password expiry: It is recommended that users' passwords be changed after a period of time appropriate to the need for protection, but after twelve months at the latest. If there is any suspicion of a possible compromise of the password, it must be changed immediately.

§3) Password Handling: The handling of passwords for *personal LRZ accounts* is subject to the following rules:

1. Passwords must be kept secret. They may not be disclosed to others or made available to them; in particular, LRZ employees will never ask for passwords either by email, on the phone or in person. See also LRZ Usage Regulations §4 (3).
2. Password entry must not be observed by others.
3. Passwords stored on computers must be encrypted.
4. Initial and reset passwords must be replaced with individual passwords before accessing the service.
5. Accounts that are no longer needed or that will not be used for a long time must be suspended.

6. Terminals used to access LRZ services and systems should, if possible, use password-protected screen savers or functionally equivalent software to prevent access to the logged-on terminal when the user leaves it or after an appropriate idle time.

Binding annotations:

1. §3 Rule 3 also applies with the necessary modifications to other authentication information, in particular private keys which are used for personal accounts in connection with SSH key pairs and (Grid) user certificates. These private keys must be protected with a passphrase conforming to the rules in §1 - §3.
2. With the necessary modifications the rules also apply to LRZ functional accounts such as are used for LRZ-hosted web services. In these cases, a limited distribution of passwords may be permissible as well as their unencrypted storage e.g. in scripts for web applications in accordance with the LRZ user administration procedures (see http://www.lrz.de/wir/kennung/). Unauthorized read-out of the passwords must be prevented by all means, e. g. by tight access control in the file system.
3. At every password change the LRZ ID Portal will check passwords against the quality criteria §1) 1.-3. (length, complexity, difference from previous password).

6 ENTRY INTO FORCE AND ENFORCEMENT

This policy was adopted by the Management of the LRZ and comes into force on 20 May 2020. Questions related to the use of passwords by users should be addressed to the respective Master User.

7 APPENDIX

7.1 FURTHER RELEVANT DOCUMENTS

The following LRZ Documents are directly relevant to this policy:

- LRZ Usage regulations, see https://www.lrz.de/wir/regelwerk/benutzungsrichtlinien_en.pdf
- LRZ article on secure handling of accounts and passwords, see https://www.lrz.de/services/security/passwords/

7.2 LITERATURE

The following literature is relevant in the context of this policy:

- ISO/IEC 27001, Annex A, A.9 Access control, particularly A.9.3.1 *Use of secret authentication information*
- BSI IT-Grundschutz-Kataloge, Maßnahmenkataloge, particularly ORP.4.A8