Appendix 1 UKRI Password Standards

UK Research
and Innovation

UK Research and Innovation (UKRI) Password Standards

UK Research and Innovation

UKRI Password Standard

Document Information

Revision History

Version	Comment	Date	By
0.1	Draft Policy created	18/09/2017	UA
0.2	Review post team meeting	05/10/2017	GN
0.3	Review post WS3 board member comments	22/11/2017	UA
0.4	Formatting changes	26/11/2017	GN
0.5	Post consultation comments	30/11/2017	GN
0.6	Post Project Board comments	06/12/2017	GN
1.0	Version approved by D&T Project Board	13/12/2017	UA
1.1	Updated 'Local IT Service Desk' to 'UKRI IT Help Desk'	20/03/2018	UA
1.2	Removed 3.2 "testpassword" as password rules are enforced by the system	30/08/18	NW
1.3	Review by UKRI Interim Head of Information Security and other UKRI/STFC staff	22/3/19	RB

Related Documents

Version	Document	Comments
1.2	UKRI Password Policy	

Document Review & Approval

Name	Version	Signature/Email Confirmation	Date
WS3 Project Board	0.6	See Meeting Minutes	05/12/2017
D&T Project Board	1.0	See meeting minutes	13/12/2017

Document Circulation / Readership

The intended circulation / readership for this document are as follows:

- UKRI Staff

UK Research and Innovation

UKRI Password Standard

Contents

UK Research and Innovation

UKRI Password Standard

1. Purpose

1.1. Passphrases/passwords are an important aspect of computer systems security. They are typically the first line of protection for user accounts. A poorly chosen passphrase/password may result in a serious breach in network and systems security resulting in:

1.1.1. Loss or exposure of potentially sensitive data

1.1.2. System compromise

1.1.3. Compromise of other network systems

1.2. All individuals including employees, visitors, contractors and vendors with access to UKRI systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passphrase/password.

2. Scope

2.1. This Standard applies to all staff who have or are responsible for an account, or any form of access that requires a password/passphrase on any UKRI system, service or technology.

2.2. UKRI staff are defined as UKRI employees, contractors, facility users, collaborators, temporary staff and secondees who use the systems, services and technology provided by UKRI.

2.3. Technology covers computers, mobile phones, tablets provided to UKRI staff and the software installed on them. Systems and services include the UKRI O365 environment, the Internet and services such as Teams, Skype for Business, Siebel, Oracle.

2.4. It also applies to any system that resides at any UKRI site, have access to the UKRI network or stores any non-public UKRI information.

3. Defintion

3.1. A **password** is a set of characters that must be used to gain access to a system. Any reference to password in this document will also refer to passphrases.

3.2. A **passphrase** is similar to a password in usage, but is generally longer for added security. It is a sentence-like string of words used for authentication, easy to remember and difficult to crack.

3.3. A **Federal ID** (e.g. network/user/login ID) is the primary UKRI user account used to access UKRI resources, such as UKRI provided systems and services.

3.4. There are other accounts which have elevated privileges, such as systems, domain and admin. This Standard also applies to these accounts.

UK Research and Innovation

UKRI Password Standard

4. Complexity

4.1. As per NCSC guidance[1], UKRI recommend the use of Passphrases and not passwords. If, for technical reasons, passphrases are not possible, then the password standard in Section 4.4 must be followed.

4.2. Your UKRI passphrase/password must meet the following complexity requirements:

4.3. Passphrase:

4.3.1. Must be a minimum of 15 characters.

4.3.2. Must contain 3 random words.

4.3.3. Must not spell a word or an abbreviation associated with UKRI.

4.3.4. Must not include words that are deemed by UKRI as offensive or rude.

4.3.5. Must not contain the login Federal ID of the account or a part of the user's name.

4.3.6. Must not contain words from the last 12 passphrases used.

4.3.7. Passphrases should only be changed in the event of the passphrase being compromised or suspected of being compromised.

4.4. If a system is unable to use Passphrases, the **Passwords** standard is:

4.4.1. Must be at least 8 characters long;

4.4.2. Must contain at least three character categories among the following:

4.4.2.1. Uppercase characters (A-Z)

4.4.2.2. Lowercase characters (a-z)

4.4.2.3. Digits (0-9)

4.4.2.4. Special characters (~!@#%^&*_-+=`|\(){}[]:;'"<>,.?/)

4.4.3. Must not spell a word or an abbreviation associated with UKRI;

4.4.4. Must not contain any common dictionary words, e.g. log-in, without some alteration to the word (see 3.3 below);

4.4.5. Must not contain the login Federal ID of the account or a part of the user's name;

4.4.6. Must be different from the last 12 passwords used.

4.4.7. Passwords should only be changed in the event of the password being compromised or suspected of being compromised.

4.5. Any attempt to set a passphrase/password that does not satisfy all the rules may be rejected. Should this happen, users will not be told why the passphrase/password was rejected.

4.6. The pound sign (£) should not be used in your passphrase/password as it is not part of the universal character set and may cause some authentication processes to fail.

4.7. Users of Apple systems should be aware that there may be issues when using UKRI Active Directory domain passphrase/passwords to authenticate services. If there are any issues, please contact your local IT Service Desk.

4.8. When a new user account is first set up (for staff or facilities users etc), your local IT Service Desk will create a random passphrase/password that will meet the passphrase/password rules. This passphrase/password must be changed by the user as soon as possible to a value that they can remember and which conforms to the UKRI Password Standards rules.

---

[1] https://www.ncsc.gov.uk/collection/passwords?curPage=/collection/passwords/updating-your-approach

UK Research and Innovation

UKRI Password Standard

5. Example of passphrases/passwords

5.1. The example passphrases/passwords below illustrate good and bad passphrase/password choices. The person's user ID is JB123:

applemoneyelephant	Example of a passphrase
applemoney2elephant	Example of a stronger passphrase by adding a number
N0wisth3win7erof0<Rd!scontent	Example of a passphrase based on the Shakespeare quote "Now is the winter of our discontent"
AbC012!"#d	This password is OK as it has the minimum of 8 characters, does not spell a word and does not include the complete user ID.
JJB123bC012!"	This password is not acceptable because it includes the user ID "JB123"

6. Changing a UKRI domain password

6.1. Your UKRI passphrase/password MUST be changed:-

6.1.1. If you know, or have any reason to believe, that your passphrase/password may have been compromised and/or become known to an unauthorised person;

6.1.2. If your passphrase/password does not conform to the current UKRI Password Standards, or if future changes to these standards mean that your passphrase/password no longer conforms to the updated standards;

6.1.3. If requested by the UKRI Head of Information Security, in accordance to the UKRI Password Policy.

6.2. You can change your UKRI passphrase/password from a system at work, remotely via a corporate service or Outlook Web Access. Please do not use the Change Password button on the Outlook login screen if you are presented with this option as this feature is not currently supported.

UK Research and Innovation

UKRI Password Standard

7. Password lockout

7.1. You will be locked out from your main UKRI account if 10 consecutive incorrect attempts are made to authenticate against any service using a UKRI Federal ID within a 30 minute period.

7.2. That account will be locked out for 30 minutes from the time of the 10th incorrect logon.

7.3. Contact your local IT Service Desk to unlock the account immediately and reset the passphrase/password.

8. Further advice

8.1. Information security training will be available and will cover passphrase/password complexity and protection. This Standard will form part of this training.

8.2. Individuals should seek guidance about this Standard or its application in their specific circumstances from their local IT Service Desk, Information Security Team or UKRI Head of Information Security.

9. Review

This Policy will be reviewed every two years or as required and endorsed by the People, Finance and Operations Committee.