University Information Management UNIVERSITEIT TWENTE.

Reference: SB/UIM/14/0131/khv
Date: 9 June 2015

University of Twente Password Policy

Contents

Summary

In drafting the University of Twente Policy Rules for Identity Management[1], the decision was taken to draw up a separate password policy in which all aspects would again be considered carefully and developed further. The different viewpoints are detailed in this document. Topics discussed are security reasons, user experience and scientific findings, which were all checked with the faculties, information security scientists and the ICTS security managers.

The Code of Conduct for IT and Internet Use[2] states that users must keep their password private. There are many different recommendations going around when it comes to password use. The value of the University of Twente password is analysed and threats are identified. The conclusion is that there seems to be little value in changing passwords for no reason.

However, the requirement that users change their password once a year remains in force. If there are any indications that a user's password has been compromised, the user must be given the advice to change it. The statements about passwords in the University of Twente Policy Rules on Identity Management are adapted accordingly.

More information must be provided about the value of passwords, about the necessity of keeping them confidential and about not using the University of Twente password elsewhere. SURFconext is used where possible for the authenticated use of external websites. Users are responsible for their own user name/password for any other websites. More information can be provided about how to deal with this responsibly, e.g. by using a password safe.

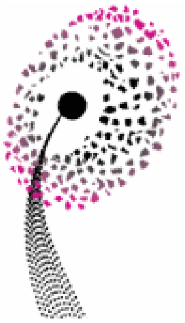
The University of Twente will in due course use multifactor authentication, for example by means of tokens or SMS. This will be based on established reliability levels. The University of Twente follows the developments at SURFnet in this regard.

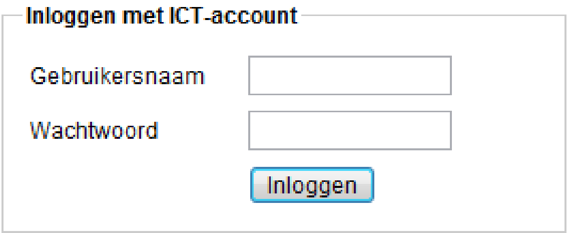
[1] University of Twente Policy Rules on Identity Management, reference SB/UIM/13/0213/khv, see http://www.utwente.nl/uim/informatiebeveiliging/Beleidsregels-Identitymanagement-Universiteit-Twente.pdf (only available in Dutch)

[2] University of Twente 2009 Code of Conduct for IT and Internet Use, see https://www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gedragscode-ict-mw-en.pdf

1 Introduction

To prevent just anyone gaining access to confidential information and to prevent information being altered by unauthorized parties, staff members at the University of Twente have to identify themselves with a user name and subsequently authenticate themselves with a password.





However, users generally do not like passwords and regularly ignore the various security recommendations. Enforced measures such as periodically changing the password are considered annoying and unnecessary. In drafting the University of Twente Policy Rules for Identity Management[3], the decision was taken to draw up a separate password policy in which all aspects would again be considered carefully and developed further. This document fulfils that role by describing the thought process. Such a detailed approach is necessary because various conflicting opinions on this subject have been voiced at the university. If just the end result is described, it will only provoke a similar response again.

Firstly, the formal rules as applicable at the University of Twente are cited and analysed. This is followed by an overview of external recommendations. An analysis is subsequently given which discusses the value of keeping passwords secret, identifies the threats and sheds light on the pros and cons of frequently changing the password. This is followed by an overview of the current situation at the University of Twente, with a brief text on the future. The document concludes with a number of policy statements.

Feedback on an earlier version of this document was provided on behalf of the faculties by Rens Brinkman, Jan Broenink and Bert Geerdink, by information security scientists Pieter Hartel, Marianne Junger, Raymond Veldhuis, Wolter Pieters, Lorena Montoya, Jan-Willem Bullée and Elmer Lastdrager and by ICTS security managers Marc Berenschot and Peter Peters. Furthermore, Aiko Pras and Stefano Stramigioli contributed key issues.

2 Code of conduct

The Code of Conduct for IT and Internet Use[4] states the following regarding the use of passwords:

> 3.3. The access key given to the user by the university is strictly personal and remains the property of the university. The access key is not allowed to be given to third parties, unless this is necessary to adequately perform the duties and only after approval from the administrator. The person who has been given the access key is required to do, or to refrain from doing, all that can reasonably be expected from him/her to prevent misuse of the access key provided.

In this article, access key is taken to mean the combination of user name and password.

[3] University of Twente Policy Rules on Identity Management, reference SB/UIM/13/0213/khv, see http://www.utwente.nl/uim/informatiebeveiliging/Beleidsregels-Identitymanagement-Universiteit-Twente.pdf (only available in Dutch)

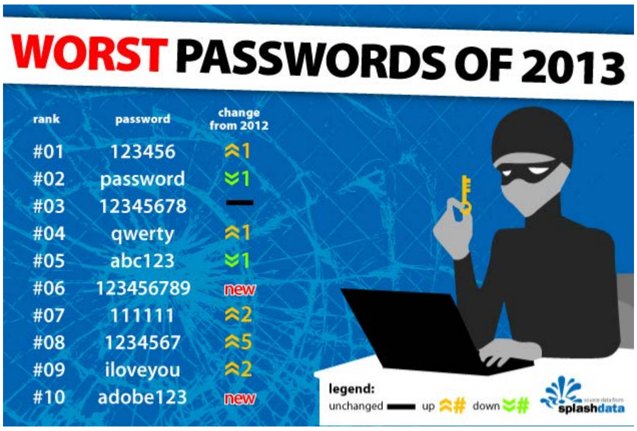
[4] University of Twente 2009 Code of conduct for IT and Internet Use, see https://www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gedragscode-ict-mw-en.pdf

2.1 Strictly personal

The University of Twente has chosen to grant access to information through the use of individual user names and corresponding passwords. This means that users should not give this information to others, but also that the systems are set up in such a way that delegating tasks is sufficiently simple and that it is therefore not necessary for users to give their login credentials to others. This applies to both the work of IT support staff and for example a research scientist wishing to delegate certain tasks to a secretary or a PhD student.

2.2 Preventing abuse

Many best practices and recommendations have been formulated to prevent the abuse of passwords. But what can reasonably be expected from a staff member? The effort to be made by the staff member will have to be weighed against the interests at stake. This will be detailed further in the following sections.



WORST PASSWORDS OF 2013

rank	password	change from 2012
#01	123456	↑1
#02	password	↓1
#03	12345678	—
#04	qwerty	↑1
#05	abc123	↓1
#06	123456789	new
#07	111111	↑2
#08	1234567	↑5
#09	iloveyou	↑2
#10	adobe123	new

legend: unchanged — up ↑# down ↓#

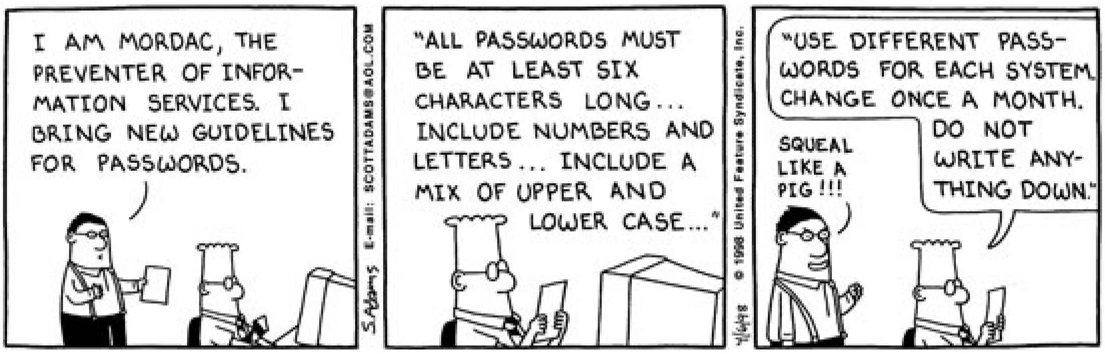
source data from splashdata

3 Recommendations

Passwords that have been leaked show that the most frequently used passwords are combinations such as ‘123456’, ‘password’ and ‘qwerty’.[5] It is abundantly clear that these passwords are inappropriate for serious use as they can be guessed easily. That is why there is usually a requirement for a minimum length and a mix of upper and lower case letters, numbers and other characters. Many general recommendations to end users on information websites such as veiliginternetten.nl (Dutch only) advocate more complex passwords and frequently changing them.

‘Veilig internetten’[6] advises changing passwords every now and again, for example once a month or once every three months. In addition, the new password must not be too predictable and should not contain consecutive numbers, for example.

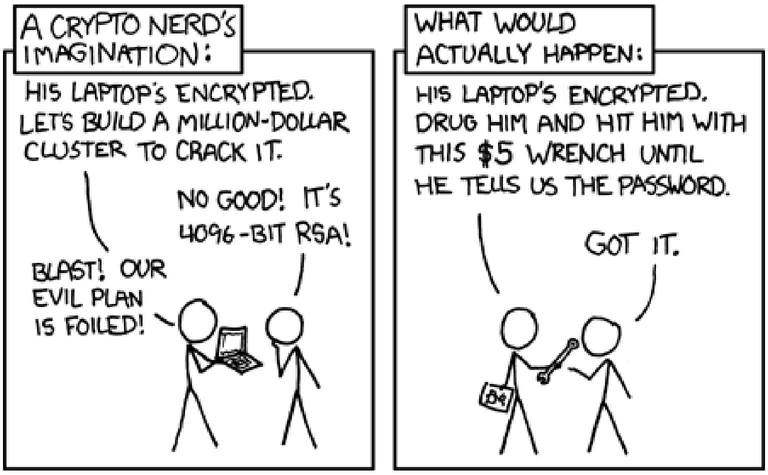
One of the Dilbert comics makes fun of this kind of advice.[7]


I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES. I BRING NEW GUIDELINES FOR PASSWORDS.
S.Adams
E-mail: SCOTTADAMS@AOL.COM
"ALL PASSWORDS MUST BE AT LEAST SIX CHARACTERS LONG... INCLUDE NUMBERS AND LETTERS... INCLUDE A MIX OF UPPER AND LOWER CASE..."
© 1998 United Feature Syndicate, Inc.
"USE DIFFERENT PASSWORDS FOR EACH SYSTEM. CHANGE ONCE A MONTH.
DO NOT WRITE ANYTHING DOWN."
SQUEAL LIKE A PIG!!!

Troy Hunt is of the opinion that a safe password cannot be memorized[8] and lists the hazards of weak passwords and of reusing passwords. He goes on to describe the possibilities that a

[5] See splashdata.com/press/worstpasswords2013.htm
[6] See veiliginternetten.nl/themes/basisbeveiliging/wachtwoorden/ (only available in Dutch)
[7] Source: dilbert.com/strip/1998-04-06
[8] The Only Secure Password Is the One You Can’t Remember http://www.troyhunt.com/2011/03/only-secure-password-is-one-you-cant.html

password safe offers users having to work with multiple passwords. Finally he sets everyone firmly back with both feet on the ground by quoting a XKCD comic[9].


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

3.1 Accountant’s advice

University of Twente’s accountant, KPMG, advises frequently changing the password. Asked to provide the rationale, KPMG responded as follows:

> “I see the standard included below as a general guideline, but in my personal view it is not a standard that should apply to all systems at the University of Twente. It is more important to me that the University of Twente itself gives thorough consideration to which settings it wishes to use. Regarding the audit for the financial statements, I would like to see that minimal requirements for a password have been considered, for instance based on the information security code.
>
> As regards good practice, I nowadays often see the following requirements:
>
> - a minimal length of 8 characters
> - lockout of 30 mins after 3 attempts
> - password duration from 90 to 180 days
> - the last 10 passwords must not be repeated
> - compulsory use van special characters (compulsory use of complex password)”

3.2 Code for information security

ISO 27002, the Code for Information Security, issues advice in §11.3.1 on how to further implement the control measure “Users should observe proper security customs when choosing and using passwords”.

> “All users should be given the advice:
>
> a) to keep passwords private;
>
> b) not to record passwords (e.g. on paper, in a file or a hand-held computer) unless this registration can be safely stored and the method of storage has been approved;
>
> c) to change a password as soon as there are indications that the system or password may have been compromised;
>
> d) to choose a password of sufficient minimum length that:
>
> > 1) is easy to remember;
> >
> > 2) is not based on something that someone else could easily guess or obtain by using person-related information such as names, telephone numbers, date of birth, etc.;

[9] http://xkcd.com/538/

3) is not vulnerable to dictionary attacks (i.e. must not consist of words that can be found in a dictionary);

4) does not contain identical consecutive characters and does not exclusively consist of numerical or alphabetical characters;

e) to change the password either at regular intervals or based on the number of times they accessed the system (passwords for accounts with special powers must be changed more frequently than normal passwords). The reuse or rotation of old passwords must also be avoided;

f) to change a temporary password when first logging on;

g) not to use passwords in automatic log-on processes, e.g. stored in a macro or under a function key;

h) not to share individual user passwords with others;

i) not to use the same password for business and private purposes."

3.3 Discussion

The accountant also mentions a number of technological measures, whereas the part copied from the Code for Information Security only deals with user conduct. Note that there is a difference between advising a user and forcing a user by technical means to observe certain customary practices regarding security. Users are smarter than any algorithm and will, if sufficiently motivated, find ways to circumvent the rules or make them ineffective. A study conducted by Microsoft Research describes this as generally rational from the user's viewpoint, on the grounds of economic motives.[10] An advice must therefore always be accompanied by a rationale, i.e. why certain conduct is desired. Advice is often provided without indicating why it is relevant, as if on a kind of need-to-know basis common in the military. A study by University College London shows that users do not follow this type of advice.[11]

4 Analysis

4.1 Value

What are passwords worth? What is the value of a University of Twente username and corresponding password? Email passwords are sold on the black market for anything between $4 and $30.[12] Significantly higher are the costs incurred by an organization which has been placed on a blacklist and can therefore temporarily not send or receive emails.

In determining the worth of login credentials, it is not the revenue for the criminal that is important, but rather the extent of the loss the user and the University of Twente could suffer if an account is compromised.

Besides the publicity damage, there are various risks that should be taken into account:

- you don't want your email account abused by spammers;
- you don't want students to be able to alter their exam results;
- you don't want someone else to alter the bank account number into which your salary is paid;
- you don't want students to be able to see the exam questions in advance;

[10] So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. Cormac Herley. Proceedings New Security Paradigms Workshop, 2009, pp.133-144. See http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf

[11] Users are not the enemy. Adams, A; Sasse, MA. Communications Of The ACM, 1999, Vol.42(12), pp.41-46

[12] See http://www.symantec.com/content/en/us/about/media/pdfs/Underground_Econ_Report.pdf

- if you have access to confidential personal information in Osiris, Oracle Applications or Decos, you want to prevent this information from becoming public;
- you don't want your research data to become public prematurely and you most certainly don't want it to be altered by unauthorized parties.

These kinds of arguments should be used in the information for users to illustrate the importance of keeping passwords confidential.

4.2 Threats

If we accept that the worth of the University of Twente password is high enough to warrant protection, are the recommendations mentioned above sensible or are these just security myths based on fiction and superstition, as Gene Spafford[13] suggests? Before any recommendations can be properly valued, it must be clear in which way a password can become compromised. Effective protection means that measures are taken against all possible threats to the confidentiality of passwords.

The NIST created a detailed map of these threats[14] and distinguishes between *theft* of passwords, *guessing* and *cracking* of passwords and *replacing* passwords.

A password stored in the browser or an unencrypted text file can be stolen if the PC is accessed, for example by a virus or if the device itself is stolen. A password being entered can be stolen by a keylogger that records every keystroke or by shoulder surfing, for example on the train when someone looks over your shoulder at your tablet or mobile. Passwords can also be stolen by social engineering, e.g. by sending a phishing e-mail and tempting users to enter their details on a website.

Guessing means repeatedly trying to find out whether a password is correct. The most common protection against this is restricting the number of possible attempts. Cracking refers to a brute force attempt using a stolen password file. The most common protection against this is hashing (and not the reversible encryption of passwords). Salting during the hashing process makes it even harder to crack a password. Advice given about password strength only works against guessing and cracking.

Passwords can be replaced by a mala fide helpdesk employee or by socially engineering the helpdesk if the organization in question does not have proper procedures in place for resetting forgotten passwords.

At the University of Twente a significant number of staff keep their password on a Post-it note near their computer screen or in a drawer. Other colleagues thus have access to it, making it easy to break the procedures for separating roles. In addition, many managers share their password with a secretary because not all systems have been set up for the option to delegate responsibilities.

The Policy Rules on Identity Management already lists many technical measures. Where possible, the University of Twente uses Single Sign On (SSO) and synchronizes the passwords for the other systems. As a result, most users only need to memorize one complex password for the University of Twente. However, there is a disadvantage to SSO: the password becomes even more valuable and if something were to go wrong, it could go seriously wrong.

The risks of phishing and the use of Post-it notes can only be overcome by properly informing users.

4.3 Periodically changing passwords

As NIST describes, regularly having to change a password is a source of frustration for users. It requires actively weighing the risks against user-friendliness to determine if it should be made

[13] Security Myths and Passwords, see http://www.cerias.purdue.edu/site/blog/post/password-change-myths/ and Passwords and Myth, see http://www.cerias.purdue.edu/site/blog/post/passwords-and-myth/

[14] SP 800-118 DRAFT Guide to Enterprise Password Management, seehttp://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

compulsory to periodically change the password and if so, which period should be chosen. As Gartner[15] remarks, the compulsory change is the most controversial aspect of a password policy. This is also the case at the University of Twente and it is the reason that the Policy Rules on Identity Management of the end of 2013 only describe the current practice for the period of changing passwords.

The idea behind frequent password changes is that if a file with encrypted passwords is stolen, the passwords must be discovered before these have changed again. However, experience has shown that most passwords are cracked within several hours.[16] Another argument is that if a user's password is leaked, it can only be abused for a limited period. In many cases, however, the password is abused immediately and this cannot be remedied by frequently changing a password. Moreover, frequently changing a password makes it harder to memorize and will often result in users availing themselves of sequential numbers and/or writing the password down.

Gartner says that if an organization opts for no-change or low-change frequency, the other processes must be set up to be robust and all precautionary measures must be taken. Even in that case, Gartner recommends an infrequent, say annual, compulsory change as a last safety net. The IDM system has been set up in accordance with this advice from Gartner.

5 Current practice at University of Twente

According to policy[17], University of Twente users have one username and Single Sign On is applied where possible. ICTS is still working on implementing this established policy. This will require users of University of Twente systems to memorize only one password. Passwords are always sent through a secure connection.

The University of Twente password will expire once a year. Users will receive notifications from a month in advance to remind them to change the password.[18] The necessity of changing the password does therefore not come as a surprise, and users are given ample opportunity to think about a new password.

5.1 Complexity

The University of Twente applies the following rules for password strength:

- A password must consist of at least 8 and no more than 16 characters.
- The new password must be different from the 3 previous passwords of the domain account and in addition must meet three of the following four criteria:
  - 1 or more special characters (!,$,#,%)
  - 1 or more figures (0-9)
  - 1 or more upper case letters (A-Z)
  - 1 or more lower case letters (a-z)

There is no opposition to these complexity requirements, although some users would like to see a longer password. Unfortunately this is technically not feasible.

5.2 External accounts

Using systems outside the University of Twente still often requires setting up a separate account. By means of integration with SURFconext, the University of Twente aims to have users

[15] Best Practices for Managing Passwords: Policies Must Balance Risk, Compliance and Usability Needs. G00201000, Gartner, 15 July 2010.

[16] See http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/

[17] See University of Twente Policy Rules on Identity Management http://www.utwente.nl/uim/informatiebeveiliging/Beleidsregels-Identitymanagement-Universiteit-Twente.pdf (only available in Dutch)

[18] See Expired password https://www.utwente.nl/en/lisa/ict/servicedesk/

log onto these external accounts using their university account. This option does not exist for a major part of external web applications. Staff and students must memorize tens to hundreds of usernames, passwords and pin codes, making the cognitive burden considerable. The University of Twente wants to keep this burden as low as possible.

By promoting the use of a password safe, users can be supported in safely storing their passwords. ICTS can provide information on the website and offer the required software to be installed. An alternative for a password safe is writing down the passwords on paper. After all, paper cannot be hacked and is understandable to everyone. That is why security gurus such as Bruce Schneier[19] and others[20] recommend writing passwords down on paper.

5.3 Users

Changing a password costs staff a significant amount of time each year, particularly if this requirement has been set on multiple devices for VPN, Wi-Fi and email. Some need support from the ICTS service desk to do so. Although there are actually no real security benefits to the compulsory annual changing of passwords, the University of Twente does not want to do away with this requirement. After all, it is advice commonly given and constitutes an existing implemented measure.

The advantage of using the same password on all University of Twente systems is that this password has to be typed in often, making it easier for the user to memorize it. Users still regularly give their password to colleagues, because not all systems are set up to allow for a delegation of tasks. That poses considerable risk. The University of Twente Policy Rules on Identity Management define the importance of setting up systems in such a way that delegating tasks is possible. Too little information is given to users about the importance of keeping their password private. The risks involved and the various scenarios of social engineering must also be highlighted. There should be no circumstance at the University of Twente in which it is acceptable to ask someone for their password.

Users want clear recommendations on how to handle their password. ICTS will have to recommend and make provisions for the use of a password safe. This will also involve discussing the risk of storing passwords on paper near the monitor or keyboard, in an unsecured text file or in the browser.

6 Future developments

In the healthcare sector, healthcare providers use a UZI card to identify themselves. At the University of Twente a digital identification card is only used to print and not to access information systems. At international level, the FIDO (Fast IDentity Online) Alliance[21] is developing standards to reduce the dependency on passwords. Parties such as Microsoft and Google aim[22] to make the use of passwords largely redundant. When operating the printers, users already identify themselves with just their own selected card, which is adequate for the chosen purpose.

In the Netherlands, SURFnet is developing multifactor authentication for cloud applications through SURFconext.[23] There are several pilot projects currently underway. A second option could be a token which assigns a code depending on the moment. Another option could be the use of SMS.

[19] See https://www.schneier.com/blog/archives/2005/06/write_down_your.html

[20] See http://www.vox.com/2014/4/16/5614258/the-best-defense-against-hackers-writer-your-passwords-down-on-paper

[21] See https://fidoalliance.org/about

[22] See http://www.theverge.com/2014/4/15/5613704/the-plot-to-kill-the-password

[23] Presentation Eefje van der Harst, Security Conference, SURFcert & SURFibo, February 2014, see http://www.surf.nl/binaries/content/assets/surf/nl/2014/presentatie-surfcert-surfibo-2014-multi-factor-authenticatie-voor-cloudapplicaties-via-surfconext---eefje-van-der-harst.pdf (only available in Dutch)

To prevent having to use different technologies for all kinds of different systems, the university has opted to work in line with the developments at SURFnet and therefore not to use supplier-specific security technology.

Some applications require little authentication. In that case, a cookie with a relatively long validity could be sufficient. Other applications, in contrast, require much more certainty about the identity of the user. In the case of a token, one prerequisite could be that the user has to collect the token in person. The Advice on reliability levels[24] discusses use-cases from Higher Education and Research (based on the HORA reference architecture).

7 Conclusion

1. The University of Twente will in due course use multifactor authentication based on established levels of reliability. The University of Twente will follow the developments at SURFnet in this regard.
2. For now, the University of Twente will continue to use passwords to authenticate users.
3. The requirement that users change their password once a year remains in force.
4. The complexity of the passwords enforced by the university is sufficient and does not need to be adapted.
5. If there are any indications that a user's password has been compromised, the user must be given compelling advice to change it.
6. More information must be provided about the value of passwords, about the necessity of keeping them confidential and about not using the University of Twente password elsewhere.
7. The University of Twente must step up its information on the possibilities of a password safe and offer the relevant software.
8. The statements about passwords in the University of Twente Policy Rules on Identity Management are adapted accordingly.

[24] See https://www.surf.nl/en/services-and-products/surfconext/what-is-surfconext/surfconext-authorisation-rules/index.html