IT Credentials Management Policy

IT Credentials Management Policy

Overarching Principle

It is the policy of the University of Strathclyde that every staff, student or other stakeholder who use the University's IT facilities should be given appropriate authenticated access to those facilities using individually assigned credentials (username and password). These credentials are created and removed by automated processes.

A complex password must be created by the user when the account is first activated. This password must be treated confidentially and not disclosed to anyone. Users can change their password whenever they wish.

These credentials will, wherever technically possible, be used to access all University provided systems and services either using common authentication or single sign-on. The University may, in addition, require an additional "two-phase" authentication mechanism on selected systems to ensure adequate security.

All access and restrictions on access will be controlled by these credentials. Each user will have a single set of credentials with appropriate levels of access whether they are staff, students or both.

Individual Responsibilities

University issued credentials provide access to a wide range of systems and services that staff and students require in order to carry out their work and study. These credentials control access to vital confidential information, to commercially sensitive information, to resources with legal and licensing restrictions, to systems that authorise financial transactions, and manage encryption on mobile devices. Thus any breach in the security of these accounts severely undermines the information security of the University. In addition it is recognised that such a breach may undermine the information security of individual staff and students.

In line with the University Policy on the Use of Computing Facilities and Resources:

- No individual may use the account assigned to another individual
- No individual should knowingly allow their account to be use by any other individual

Some users may consider sharing their credentials to accommodate their normal business processes – e.g. in a manager/PA situation. **This is never acceptable**; there are technical solutions available which allow these modes of working to take place without divulging passwords.

In the event that an individual's account is compromised (i.e. the password being known to anyone) they must change their password immediately or request that Information Services disable the account (contact help@strath.ac.uk) until the password can be safely changed.

The University requires its staff and post-graduate research student account holders to change their password at least **once a year**. It advises that undergraduate and post-graduate taught students change their passwords annually.

Accounts for Staff and Students

The creation and removal of accounts is automatically controlled via the HR system (for staff) and the Student Record System (for students).

Arrangements for staff on leaving the University are covered by Policy on IT Access for Leavers.

Student accounts are removed several months after they graduate or leave the University. Warnings are provided before the accounts are finally removed.

Business Continuity Arrangements

It is recognised that occasionally it is necessary to access a member of staff's account after they have left for business continuity arrangements. Such access is governed by the Procedure for Accessing Personalised Electronic Storage Resources. For this reason staff accounts are retained in an inaccessible, "dormant" state, for six months after the staff member leaves.

If a staff member leaves and returns within the six month period, their account will normally simply be reactivated.

Temporary or Limited Accounts

The University offers two different types of accounts on a temporary basis.

Temp IT Access Accounts

These are issued to people who will need full access to IT facilities such as an email account and/or a network login.

Limited Access Accounts

These are issued to people who need access to one application such as MyPlace or Sharepoint. Such people are generally external collaborators who will have email and network access provided by their own employer.

Both are requested by appropriately authorised staff (usually Faculty/Department IT staff) or via the Helpdesk. They are created and managed via online application systems. This also sets expiry dates on the accounts, although accounts can be extended via the relevant system by the sponsor or the person who made the request.

WiFi Arrangements for Visitors

It is unnecessary to issue credentials to visitors purely for accessing WiFi. Visitors from other academic institutions will generally be able to use eduroam and their own credentials as issued by their home institution. Other visitors can create accounts for themselves on the campus visitors' network (currently _The Cloud). See http://www.strath.ac.uk/it/infrastructure/networking/wirelessaccess/

The Right to Suspend an Account

The University of Strathclyde must ensure its own Information Security and that of its staff and students. For this reason it reserves the right to suspend without notice any staff, student, Temp IT Access, or Limited access account. It also reserves the right to suspend without notice access to any system or service, or a component of such a system or service.

Role Accounts

For certain types of business operation it is necessary to have a "role account". This is a non-personal account that is used by several people to fulfil a single business function. An example would be the account help@strath.ac.uk used by the ISD Helpdesk. There is no personal information or personalised access rights associated with such an account.

Anyone requiring such an account should contact the ISD Helpdesk and complete an "Application for Role Account" form. They then are recorded as the sponsor of the account and become responsible for ensuring the legitimacy of its use.

The sponsor can then provide the details of the account to the staff members who require access to it to fulfil the business function. The sponsor must retain a list of all individuals who have access to the account and all such individuals must be employees of the University of Strathclyde. When anyone leaves or changes roles that had access to a role account the sponsor must change the password on the account to ensure that no one can access the account that no longer requires it.

Should the sponsor of a role account leave or change role they should arrange a new sponsor for the account and notify the ISD Helpdesk prior to leaving/changing roles. In the event an account no longer has a sponsor the Head of Department will be asked to nominate a new sponsor if the use of the role account is to continue.

When requesting role accounts it is important that the sponsor considers the email address that will be associated with the account. The email address requested cannot always be provided. It might already be in use, it might have an ambiguous meaning and abbreviations can have multiple meanings both within and outwith the University.