Policy for Temporary IT accounts

Version Control and History

Title	Description	Author	Approved by	Date Approved
Policy for Temporary IT Accounts Version 1.0	Policy for the management of Temporary IT Accounts	User Accounts Management Group (Information Services Directorate)	Information Strategy Committee	4/10/2023

1. TEMPORARY IT USER ACCOUNTS – GENERAL POLICY DETAILS

1.1 What is a TEMP (Temporary) IT user account and what levels of access are provided to IT systems?

A Temp IT account is a University user account sponsored by a staff member within the University for an external partner/associate who is not an employee or student at the University.

Temporary IT access is requested, sponsored, and managed entirely online via the Temporary IT access service within Pegasus. Temporary IT access is managed by approved account administrators across the University.

A Temp IT account has a default time period of up to 1 year and will provide the user with:

a) A University DS account that allows restricted access to various University systems such as Library Services, the University's staff and student portal (Pegasus) and the Virtual Learning Environment (Myplace).
b) A University @strath.ac.uk email address on the University's Microsoft 365 Email service and membership of the University's directory lists
c) Access Eduroam that allows the user to connect to the University's WIFI network when on campus
d) Access to all other Microsoft 365 online services and MS services with an A1 level access: for example, Microsoft Teams, One Drive, SharePoint, Skype for Business
e) An H Drive - individual file storage on University systems
f) The University's Virtual Private network (VPN)
g) Permission to request Zoom – a collaborative working tool
h) A Unique person ID record on the corporate system containing personal information which allows their record to be used within corporate systems.

Temp IT accounts **are not licensed** for:

a) Access to online External library/Research e-Resources
b) Software downloads.
c) Access to Specialised software tools licensed for staff and students only
d) Corporate Financial, HR payroll, Estates, Student Records or Research Management Systems
e) Strathclyde virtual desktops

1.2 Who is eligible for a Temp IT account?

Typically, the following associate types are eligible for a Temp IT account for the following functions:

Associate type	Associate type
Academic Visitor Administrative Support Adult Trainee Agency Temps Consultancy Services Consultants Contractor DemonstratorExam Scribe Exam Scribe (Extra Provision) External Assessor External Examiner (PGR) External Examiner (PGT) External Examiner (UG)	Honorary Staff Invigilator Invigilator (Extra Provision) Lecturer (Guest) Marker Mentor Personal Support Assistant Practical Lab Assistant Researcher Scribe/Note-taker Study Support Assistant Telethon Tutor

Temp IT account administrators should assess the requirements of the individuals before setting up a Temp IT account for a new user as often a Limited access account will be sufficient for the purposes of engagement with the University. Temp IT account administrators should refer to and be familiar with Information about user accounts and specifically of the Types of user accounts and access to ensure they are setting up the right levels of access with the right account type.

1.3 Roles and Responsibilities for managing the account

Requestors : These are staff requesting access for an external associate. Typically, they are administrative staff within a department, but anyone can request a Temp IT account online.

Sponsor : Temp IT accounts must be sponsored by a staff member within the University who has a working relationship with the intended account user and their organisation (where applicable). The sponsor must be able to vouch for the account user and carry out due diligence checks. Sponsors are responsible for managing the relationship with the external person and authorising account set up, changes and early closure of the account when the access is no longer needed.

Account User : The intended user is responsible for the provision of personal information for account set up, signing up to terms and conditions of use and notifying the University (e.g., their sponsor) when they no longer require access or require an extension.

Temp IT Account Administrators: are responsible for the assessment of the requirements for the account type, set up and management of the account under the direction of the sponsor including activation/deactivation of the account and extensions to time periods of use. Temp IT account Administrators are typically Faculty IT staff for requests originating in the faculties or Helpdesk staff for requests originating from professional services.

All parties need to read and understand the University's Data Protection Policy, the Information Security for Staff policy and Legal Framework for ICT; and will be asked to accept terms and conditions the first time they use the service.

More details of roles and responsibilities are provided in sections 2-5.

1.4 Cyber Security, Breaches, and Data Protection in relation to the account

The University must provide information to trace individuals using our systems should a security breach or cyber incident occur with the account. Strathclyde (ISD) will deactivate the account in the event of a security or data breach that is related to the account. The University will conduct a security incident investigation and identify any appropriate actions for Strathclyde and/or the User. The University will take any actions it deems necessary in accordance with its obligations under data protection legislation.

For that reason, and for account administration purposes and the prevention of duplication of person records on our systems, the University requires to collect a certain amount of personal information from the user including full name, date of Birth (DOB), Personal/External email, Mobile number, and home or organisation address. Where applicable, name and address of the affiliated organisation that the user represents should be supplied.

1.5 Automated workflows and system processes in relation to the account

Several workflows and automated processed with email will be initiated on the set up and activation of the account and management of the account thereafter. These primarily are for new accounts:

a) **Requestor → Sponsor** : On successful submission of a new Temp IT access request, an email will be sent to the sponsor to allow them to review and authorise/reject the request.

b) **Sponsor→ Account User:** On sponsor authorisation, an email will be automatically sent to the user's personal email address with a link to supply personal details necessary for cyber security and person matching. This has a timeout on it.

c) **Account User→ Account Administrator**: On successful submission of the Pegasus form by the user, an email will be sent to the Temp IT account administrators to allow them to process the full request. This will include electronic matching to existing records - the user's personal email address will be validated to ensure it is unique to the account and not shared with other user accounts. The administrator can authorise or reject the request. The authorisation initiates the creation/update to the user account.

d) **User Database→** Account **User**. The user is sent an email with username details and a link to the password reset.

e) 'Terms and conditions' online agreement will be required to be 'signed' by the user when they first login to Pegasus after their password reset.

f) Account Users and Sponsors are notified of the account's termination one month before the end date.

Similar processes are available to extend access for existing Temp IT accounts beyond the end date specified.

2. Responsibilities of the Requester

2.1 Limited access request versus Temp IT request

The requestor should ensure that access is provided on a 'needs' basis and in most cases, a Limited Access Account will meet the user's needs. If the requestor is unsure which type of account to request, then the web site provide information for User account types .

2.2 Initiating account set up

As the initial instigator of the request, the requestor is tasked with providing accurate online information in relation to the request for basic personal information to the account administrator for the preliminary account set up including

a. Forename, Surname
b. External email address
c. Postal Address (home or Organisation)
d. Affiliated Organisation name (if applicable)
e. Reason for access
f. Start and End date of the access
g. Providing the sponsor details for the request – this must be the staff member who has the relationship with the external person.

3. Responsibilities of the Sponsor

3.1 Authorising/ rejecting the account creation

The sponsor must process the request to either authorise or reject the request via Pegasus.

As the primary contact and 'relationship' manager, the sponsor must have an active and verifiable relationship with the external associate. If the sponsor has no relationship with that person, then they must reject.

3.2 Authorising extensions to length of time for usage.

The sponsor must authorise account extensions online on Pegasus if the account user still requires access beyond the end date.

3.3 Manage the relationship with the Account User

The sponsor must

a) Terminate the account or notify the account administrator of early termination of the relationship/account access e.g., the user has left the organisation they work for
b) Request an extension online if the account access if required beyond 1 year
c) Notify the account administrator of changes to the organisation the user works for that impact on the information held against the user e.g., organisation name change

3.4 Training

The sponsor is required to arrange where necessary appropriate information/training/contacts for the user for using IT systems/University processes.

3.5 Cyber security and data protection

The Sponsor must be aware and have read and understood the University's Data Protection Policy and the Information Security policy and the Legal Framework for ICT document.

The sponsor should notify the University of any security breaches they have become aware of that relate to the account.

If the University arranges a formal contract with an affiliate organisation that requires members of that organisation to have access to University IT systems, then a formal agreement/contract with them must include a Data Processing/Sharing agreement as part of the contract. For more information, please contact dataprotection@strath.ac.uk

4. Responsibilities of the Temp IT Account User

4.1 Provision of personal information

The Account user must verify/provide via a secure online link the following information to allow person matching and for security reasons.

a) Full name
b) DOB
c) Mobile number
d) Postal address

4.2 Sign up to terms and conditions in relation to IT policies

As part of the user's first login, the Account user must read and understand the University's Data Protection Policy and the University's Information Security Policy .

4.3 Security and Multi factor authentication

The Account user must

a) Set complex passwords and regularly update passwords
b) Use Multi factor authentication mechanisms for example by using the MicroSoft Authenticator app
c) Report any security/data breaches that they are responsible for to the University.

4.4 Inform the University of changes to their status with the University

If the Temp IT account user no longer requires access e.g., they are leaving the affiliated organisation, then they should inform the University.

5. Responsibilities of the Account Administrator

5.1 Limited access versus Temp IT account

On receiving a request to authorise, the Temp IT Account administrators should double check and assess the requirements of the individual before setting up a Temp IT access for a new user as often a Limited access account will be sufficient for their purposes of engagement with the University. IT Temp Account administrator should refer to and be familiar with Information about user accounts and specifically to Types of user accounts and access documentation to ensure they are setting up the right levels of access with the right account type.

Having assessed the requirements for the need for a Temp IT account as opposed to the Limited access account, the account administrator should authorise/reject.

5.2 Set up and manage the Temp IT account

The Account Administrator is responsible for

a) Reviewing the details of the request to check all information is in order and in particular, the details supplied by the account user.
b) Perform person matching for potential matches to prevent duplicate entries being entered.
c) Authorise /Reject Temp IT requests for new accounts or for accounts that require extension
d) Deactivate accounts where the user is no longer an associate of the University – normally under the sponsor's direction.
e) Monitor the overall provision and status of IT Temp accounts in their area.

5.3 Cyber security and data protection

The Temp IT Account Administrator is aware and has read and understood the University's Data Protection Policy and the Information Security policy and the Legal Framework for ICT document.

The Systems Administrator should notify the University of any security breaches they have become aware of that relate to the account.