Information Management and Technology: Internal and External User Access Procedure

1. Guiding Principles

This procedure has been developed to ensure that all aspects of user access to the Health network and terminations of users from the Health network in a timely manner are identified and followed throughout by the WA Country Health Service (WACHS) Information and Management Technology (IM&T) departments in all regions

2. Procedure

All WACHS sites are to use the electronic health form number 30 (eHFN-030). This form must be filled out by the applicant's line manager for them to be assigned a health employment (he) number and access to the Health computer network and systems.

All eHFN030 completed forms can be accessed from HPSM or the Access Request website.

Where an employee is on a fixed term contract, it must be indicated on the eHFN030 form by the requestor. The eHFN030 must have the start and end date specified, and the Employment Type field must be set to contractor

2.1 New Starters

- All new starters must register their acceptance of the 'Acceptable Use Policy' via the health point 'My Contact Details' web page located at: https://healthpoint.hdwa.health.wa.gov.au/Pages/default.aspx.
- Line Managers are responsible for ensuring that new staff members read and accept the Acceptable Use Policy (AUP) within 14 days of the account being used for the first time.
- Failure to accept the AUP within the 14-day time frame will result in the account being automatically suspended.
- Line Managers will receive an email outlining the basics details of the new staff members accounts. They are to print this out and supply it to their new staff member when they commence work.

2.2 Change of Access

- An eHFN030 is required before WACHS IM&T will process any modification to a client's access level. This applies to data and information access systems.

2.2.1 User Transfer

Where an eHFN030 request is received for a user transferring between regions or HSPs, the eHFN030 request will be forwarded to the User Provisioning Officers (UPO) team in the departing Region or HSP to begin the transfer process.

The UPO team in the departing region / Health Service Provider (HSP) will:

- remove all permissions no longer required, including any licences applied via security groups.
- move user data to the “User Transfer Folder”
- if the user is transferring to Central Office or another HSP, move the users Active Directory (AD) account to the “User Transfer” OU, otherwise the account can remain in the WACHS OU.
- on completion of the above work, reassign the request to the new HSP or WACHS region UPO team.

The UPO team in the region / HSP the user is transferring to will:

- apply all relevant permissions
- relocate user data from the “User Transfer Folder” and configure for the appropriate location
- complete the HPSM request.

2.3 Terminations

- WACHS IM&T Security will ensure actions outlined in the monthly security task list are completed.
- WACHS IM&T Security will provide regional IM&T and Regional Health Information Managers (HIMs) monthly reports that outline disabled accounts which have access to core clinical applications.
- WACHS IM&T Security will disable user accounts that have not been used in 90 days or more.
- WACHS IM&T Security will use the HR Termination Report to identify accounts of former employees and perform a monthly termination procedure to disable those accounts.
- WACHS departmental managers are responsible for ensuring both the T1 and T2 forms are completed in a timely manner in line with WACHS Employee Cessation Policy.

2.4 External Vendor Access requests

- WACHS Managers are to ensure that non-health identities that require access to the Health Network, complete the HFN060 and HFN057 forms.
- Where an external vendor is a medical service provider, access to clinical applications will be granted as agreed upon between WACHS and the external vendor.

- Access to clinical applications not specifically listed in the HFN060 will not be provided. Access to extra clinical applications will need to have a modified HFN060 signed off prior to access being provisioned.

2.5 User Accounts

- WACHS user account login passwords must comply with the WA Health password standard which is a passphrase of minimum 10 characters and two or more words.
- Password complexity is enforced by active directory configuration and is subject to change.
- WACHS user accounts must not have a non-expiring password set.
- WACHS user accounts must not have the “password not required” option set.

2.6 Privileged Accounts

- Privileged accounts must be denoted with an “a” on the end of the account name
- WACHS privileged account password must differ from the standard user account password owned by the same User.
- Privileged accounts passwords must align with the WA Health password standard
- Privileged access accounts and groups must be reviewed by regional IM&T teams as part of monthly security reporting.

2.7 Service Accounts

- Service Accounts in WACHS should follow Vendor best practice where feasible.
- Service Accounts must have passwords that align with the WA Health Standard
- Service Accounts are not to have Internet access unless necessary for them to perform their required task. Those that do require internet access should be restricted to required URLs and Ports.
- A HPSM change should be logged by regional IM&T to record that the password change has occurred.
- The Active Directory (AD) account must have the associated HPSM reference number included in the AD description field.

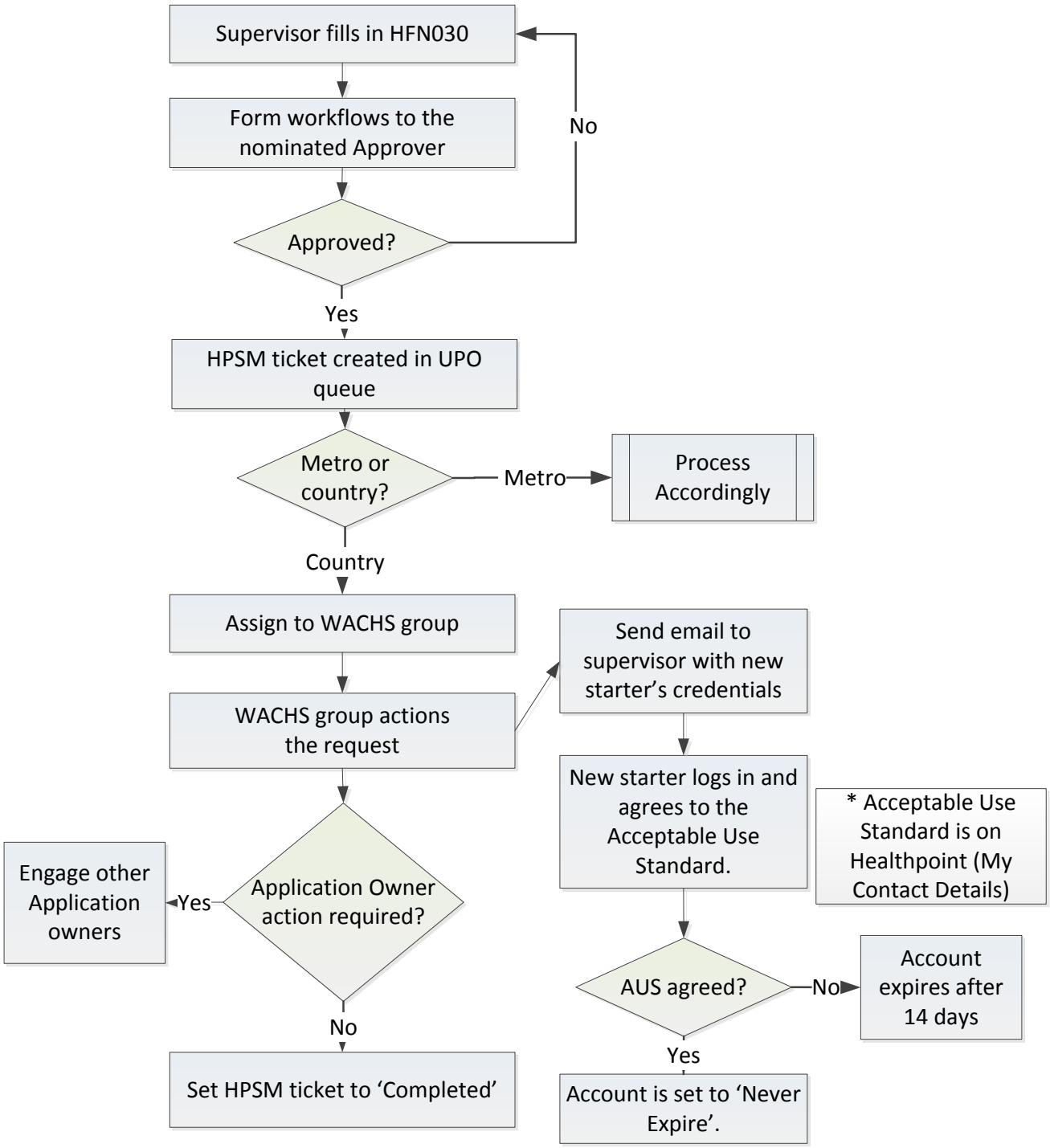
2.8 Generic Workstation Accounts

- Requests for generic workstation accounts (GWA) must be submitted via the eHFN-030 form.
- Authorised Approver must be of Tier 3 or above, and be willing to meet the requirements as defined in the Information Security policy
- GWAs must not have access to the internet.
- GWAs must not be provided access to applications containing clinical / patient data.
- GWAs will not be permitted access to folders contained in the W: drive on the WA Health network.
- GWAs will only be permitted access to applications that have been approved in the eHFN-030.
- Passwords for GWAs must be reset in line with the WA Health password standard and complexity rules.
- Regular monitoring and auditing of GWAs must be performed by the authorised approver to ensure the account is only being used for its intended purposes.
- GWAs are to be restricted to specific computers via the use of the Active Directory “Log On To...” function.

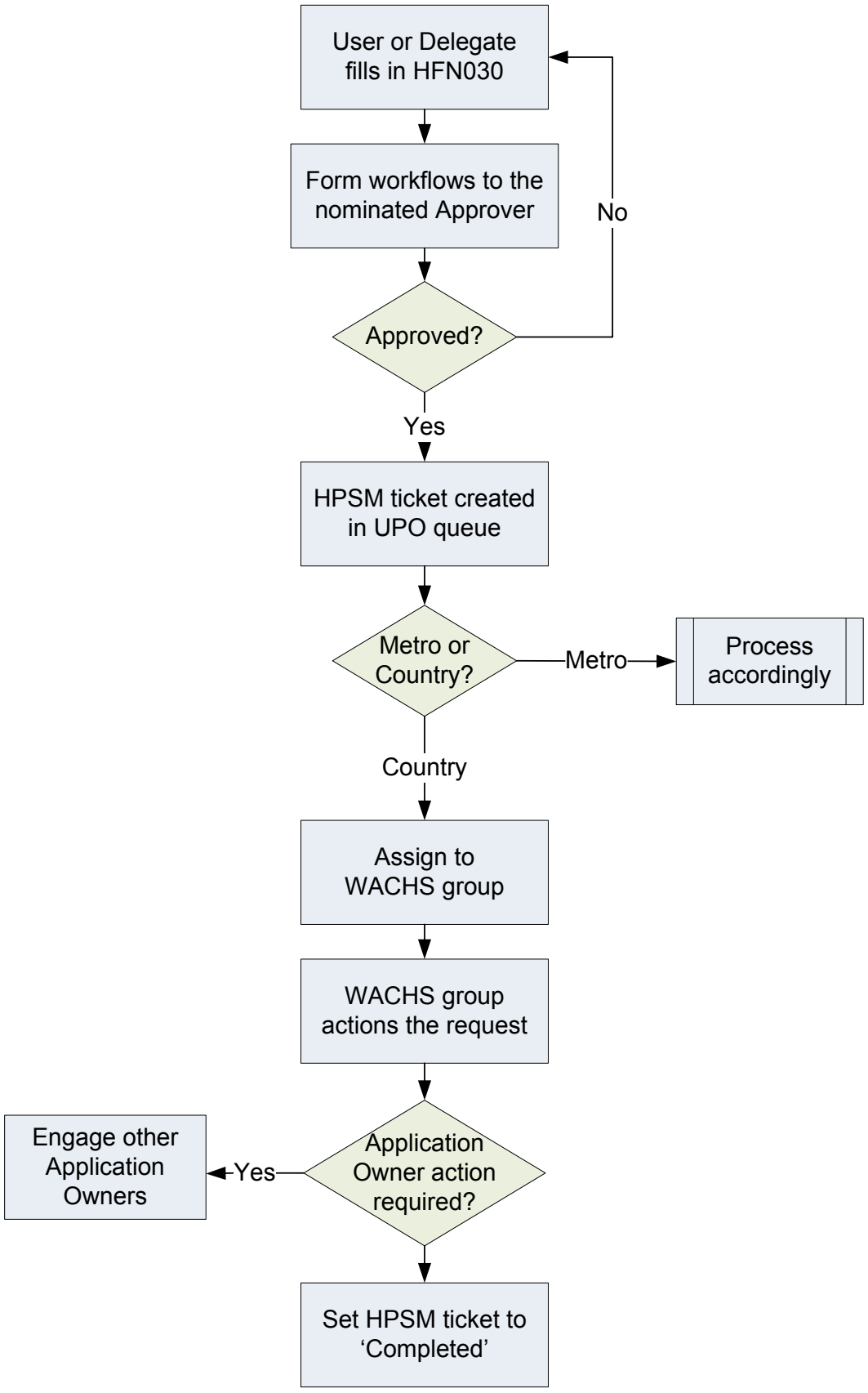
2.9 Shared Mailboxes

- Requests for shared mailboxes (SM) must be submitted via the eHFN-030 form.
- Initial list of users to have access to mailbox must be in the submitted eHFN-030 form.
- Subsequent user access to a shared mailbox must be via an eHFN-030 submitted for the user needing access.
- “Send As” permission is not to be granted by default. It must be specifically requested, with approval provided by the Head of Department.
- User accounts that were created as part of the shared mailbox creation process are not to be used as pseudo generic workstation accounts.
- These accounts are to be marked as Shared Mailbox Accounts (SMA), disabled, and to have a password set that is not shared with users.
- SMAs which are to be used on mobile devices are to be accessed via the Outlook App.

WACHS New starter process



WACHS 'Change my' / 'Change others' access process



3. Definitions

Form used to request access to Health network facilities by Health employees. Applications may have their own request for access form.	HFN-030
Agreement to Network Access by an external organisation.	HFN-060
Request for Network Form for employees of external organisations who have a HFN-060 in place.	HFN-057
HSS provides corporate shared services to the Department of Health and other health agencies that comprise the Health Shared Service Cluster.	HSS
IM&T service ticketing and inventory management tool.	HPSM
ICT Service Delivery and Operations was established to drive the Information, Communications and Technology reform program, provide a focus on the importance of health information in our system and enable efficient and integrated technology services.	HSS-Service Delivery

4. Roles and Responsibilities

This procedure is to be adhered to by all WACHS Employees and External Service Providers requiring access to Health Information Systems.

5. Compliance

This procedure is mandatory. Failure to comply with this procedure will constitute a breach of the Acceptable Use Policy – Information and Communication Technology, and the WA Health Code of Conduct (Code).

The Code is part of the Integrity Policy Framework issued pursuant to section 26 of the *Health Services Act 2016* (WA) and is binding on all WACHS staff which for this purpose includes trainees, students, volunteers, researchers, contractors for service (including all visiting health professionals and agency staff) and persons delivering training or education within WACHS.

Exemptions
If it is not possible to meet one or more of the requirements in this procedure a HPSM request must be submitted requesting an exemption and assigned to WACHS IM&T Security. Exemptions require approvals from a relevant tier 3 manager.

A formal risk assessment will be conducted by WACHS IM&T Security. The findings of the risk assessment will be provided to the requestor. The requestor must then seek approval for exemption from a relevant tier 3 manager via a briefing note (BN). The signed BN should be sent through to WACHS IM&T Security for filing. The exemption will then be granted.

The HPSM request should then be updated by WACHS IM&T Security with a final note outlining the specifics of the exemption.

The Active Directory(AD) account must also include the associated HPSM reference number in the AD description field for the approved exemption.

6. Records Management

All WACHS corporate records must be stored in the approved Electronic Documents and Records Management System in accordance with Records Management Policy.

7. Evaluation

Monitoring and reporting is undertaken by WACHS IM&T Security.

WACHS IM&T Security will produce monthly a Termination report which will identify users which they have removed their access to the Health Data network.

WACHS IM&T will provide a Termination report to Health Information Managers (HIMs) and the Financial Team. HIMs and the Financial team are to remove access for users identified in the report

8. Standards

National Safety and Quality Health Service Standards – 1.7.c, 1.8.a-c, 1.16c, 1.18.c
Health Support Services - Health Password Standard (in development)

9. Legislation

Health Services Act 2016 (WA)

10. References

Nil

11. Related Forms

Electronic HFN030 Forms
HFN060 Deed of Agreement for Network Access
HFN057 Request for Network Access

12. Related Policy Documents

WACHS Cessation of Employment Policy

13. Related WA Health System Policies

MP 0066/17 Acceptable Use of Information and Communications Technology Policy

14. Policy Framework

Information and Communication Technology

This document can be made available in alternative formats on request for a person with a disability

Contact:	Area Manager ICT Operations		
Directorate:	Innovation and Development	**EDRMS Record #**	ED-CO-13-65455
Version:	4.00	**Date Published:**	23 March 2021