End-User Device Rules

Provisioning and Deprovisioning

1. End-user devices must be provisioned and maintained centrally, and must have, at a minimum, the Crowdstrike Falcon EDR agent and any other required scanning or security agent installed.
2. WHO authorized or provisioned end-user devices which have not been used to sign in to WHO on-premises or cloud systems for over 30 days must be disabled, unless there is an exception approved by the director of HRT.

Local Administrator Permissions

Technical and Process Ownership:

3. The Operations and User Support (OUS) and Workspace Collaboration Services (WCS) are technically responsible for the management and implementation of local administrator permissions. This involves configuring and managing technological solutions, establishing monitoring, and logging systems, and ensuring adherence to the outlined cybersecurity controls.
4. Local Administrator Permissions Request Process:
    a. Formal Request Submission: Workforce members must submit a formal request for local administrator permissions through the designated request form in MyService.
    b. Business Justification: The request must include valid business justification and be submitted to the immediate supervisor for initial approval. Please see the Guidance for Approvers on Justifications for Local Admin Permissions document.
    c. Exception Handling: Establish a clear process for handling exceptions, including higher-level approvals and additional scrutiny for any deviations from the standard process.
5. Approval Process:
    a. Supervisor Review: The supervisor must review the request and assess the necessity of local administrator permissions for the workforce members' role. By approving the local admin permissions, the supervisor acknowledges and understands the cybersecurity risks involved with granting such permissions.
    b. Multi-Level Approval: Approved requests by the supervisor are then forwarded to Operations and User Support (OUS) for further evaluation and final approval.

Permission Assignment

6. Time-Bound Permissions: Once approved by OUS, local administrator permissions will be granted for a specific duration, not exceeding one month.
7. Acknowledgement of IT Policies: Individuals must confirm receipt of these permissions and agree to adhere to the Global Cybersecurity Policy and any additional guidelines provided.

Technical Controls:

8. Temporary Access Management: Implement technology to provide just-in-time (JIT) access, ensuring local administrator permissions are granted only for the necessary duration and automatically revoked afterward.
9. Monitoring and Logging: Enable detailed logging and monitoring of activities performed with local administrator permissions. Any deviations from normal behavior should trigger security alerts to the Cybersecurity Team (CST).

Review and Revocation:

10. **Monthly Review**: Organizational units must, using data provided by OUS, conduct a monthly review of all workforce members with local administrator permissions.
11. **Necessity Reassessment**: The necessity of continued permissions will be reassessed, and unused or unnecessary permissions will be revoked.

Workforce Responsibilities:

12. Responsible Use: Workforce members who are granted local administrator permissions must use them responsibly and adhere to the Global Cybersecurity Policy in eManual.
13. Prohibited Actions: Workforce members must not share their credentials or use them to perform unauthorized actions.
14. Incident Reporting: Any cybersecurity incidents or suspicious activities must be reported to the Cybersecurity Team (CST) immediately at cybersecurity@who.int.

Additional Controls:

15. Documentation and Audit: Maintain comprehensive documentation of all permissions granted, including justifications and approval records for the request.
16. Training and Awareness: Conduct regular training sessions and awareness programs to educate the workforce about the risks associated with local administrator permissions and best practices for cybersecurity.
17. Feedback Loop: Implement a feedback mechanism where workforce members can report any challenges or suggestions related to the local administrator permissions process, allowing continuous improvement of the guideline.

Bring Your Own Device

18. The use of personal devices for official business at WHO is permitted exceptionally when their owner agrees to accept a degree of control and visibility by WHO under these rules.
19. Personal devices used for official business must have the Crowdstrike Falcon agent installed and configured for monitoring by the WHO Security Operations Centre.
20. The owner of personal devices must agree to permit admin access for WHO to, at a minimum, control that data on the device which results from interaction with WHO system.

Safe Disposal of Electronic Equipment

21. The purpose of this rule to establish standard way to protect WHO information when an item of electronic equipment is re-used or discarded.
22. Each WHO location that has ownership or custodianship of any electronic equipment must create and maintain an inventory of all devices. At a minimum this must contain the following information:

    - Serial number
    - Device type
    - Physical location
    - Owner
    - Individual or Division to whom device is assigned. If the equipment is located in a data centre then the name of the data centre.
    - Date of placed in service
    - Anticipated end-of-life date
    - Date of destruction
    - Certificate of destruction

23. The device inventory must be maintained and kept current. This particularly applies to the physical location of assets.
24. Once an asset has reached its end-of-life in its current location, its disposal must be planned. There are two possibilities for disposal:

    i. Destruction

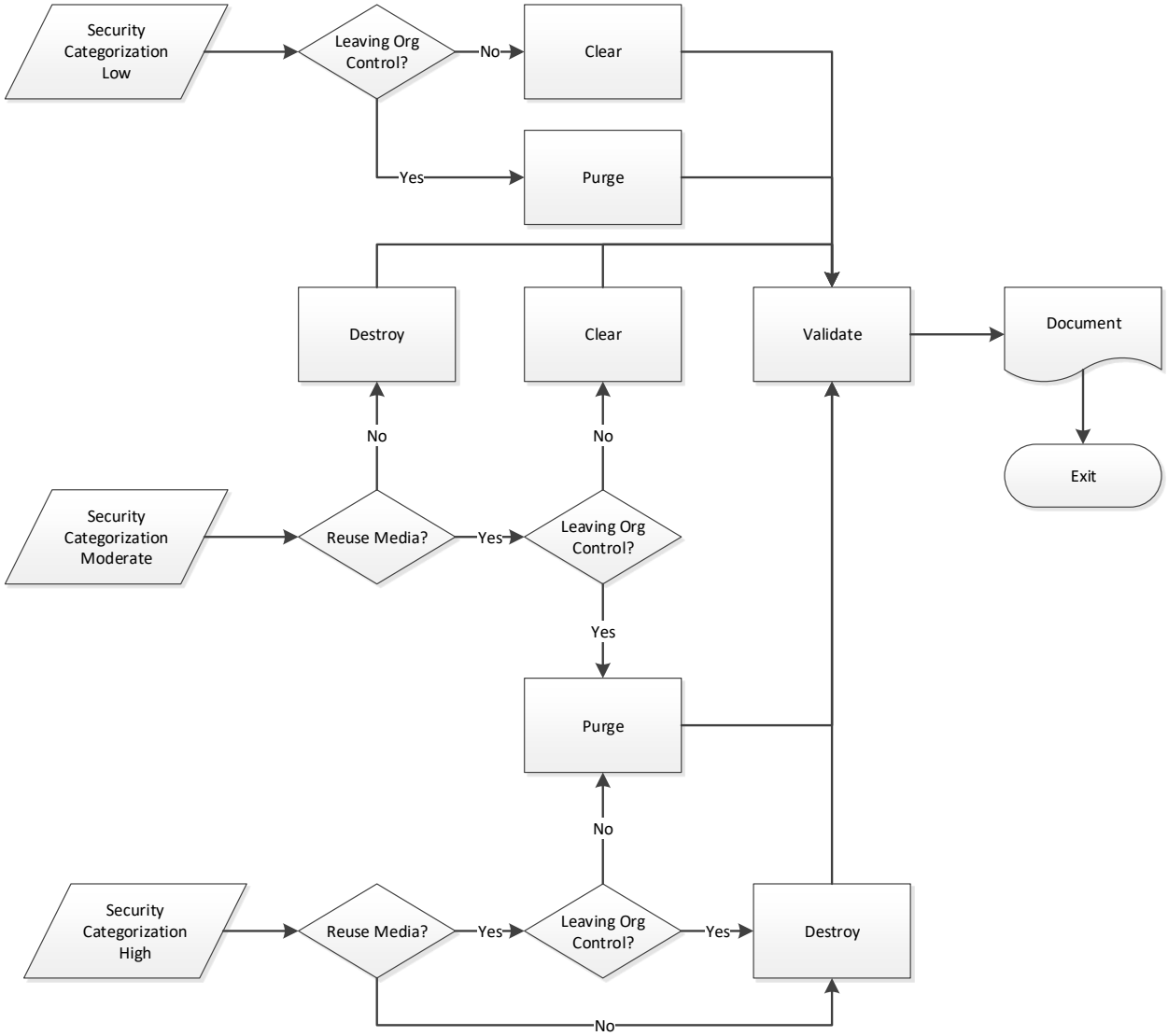
    ii. Re-use (either within the WHO or externally if this is approved local practice)

25. The decision about how to dispose must be recorded in the asset register.
26. Regardless of whether the equipment is to be re-used or destroyed, any storage component of the media must be subjected to a Sanitization procedure. Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:
27. Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

iii. Purge applies physical or logical techniques that render Target Data recovery infeasible using state-of-the-art laboratory techniques.

iv. Destroy renders Target Data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data.

28. Media sanitization is a process by which information is irreversibly removed from the media. The low, moderated, and high security categorizations are related to the type of risk to WHO. The security categorization Low is equivalent to low risk. The security categorization moderated is equivalent to medium risk. The security categorization high is equivalent to high or very high risk. The WHO risk is calculated by the Cybersecurity Risk Framework Tool at link. The below flow diagram determines the level of sanitation to be applied:



29. Media Sanitization by “clearing” or “purging” must be performed on site at WHO before the media reach the service provider for media destruction. NAID-AAA-certified / NIST 800-88 compliant service provider for media destruction are allowed to perform the sanitizing and destruction off-site. The service provider for media destruction must issue a certificate of media destruction. A copy of the certificate of destruction is to be kept in the IT inventory storage.
30. Media containing sensitive data must go through an adequate secure erase before being re-issued. Multi-pass secure erase is not required when the destruction renders the target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data.
31. Media that has undergone secure erase must be verified before shipment to the service provider.
32. Service Providers that store WHO data in the cloud need to comply with the WHO policy of secure disposal of electronic equipment.

Definitions

33. Destroy - A method of Sanitization that renders Target Data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data.
34. Clear - A method of Sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
35. Validate - The step in the media sanitization process flowchart which involves testing the media to ensure the information cannot be read.

CERTIFICATE OF SANITATION

PERSON PERFORMING SANITATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*	
Classification:	Data Backed Up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITIZATION DETAILS		
Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct		
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other:		
Method Details:		
Tools Used *(Include version):*		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)*		
Details:		
SIGNATURE		
I attest that the information on this statement is accurate to the best of my knowledge.		
Signature:		Date:
VALIDATION		
Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date: