



Office procedure

Date: 18 January 2021

End-user computing devices

Introduction

1. This Procedure establishes the processes and procedures to ensure that individuals working at the ILO have the appropriate end-user computing devices to effectively perform their duties. It supersedes Office Procedure, *End-user computing devices*, IGDS No. 497 (version 3), of 18 November 2019.
2. The Information and Technology Management Department (INFOTEC) is responsible for defining standards and practices for hardware and software deployed throughout the Office.
3. End-user computing devices (IT devices), including personal computers (PCs), laptops, smartphones and tablets are essential tools which facilitate the work of the Office.
4. Users of IT devices should be aware that access to the ILO systems from IT devices is monitored for appropriate use.
5. ILO systems include the ILO intranet, ILO Wi-Fi, ILO desktop software, IRIS and other applications, email, Skype, shared network drives, etc.
6. This Procedure should be read in conjunction with:
 - (a) Office Directive, *The use of email and Internet in the ILO*, IGDS No. 452;
 - (b) Office Procedure, *Accessing the ILO network*, IGDS No. 496; and
 - (c) Office Procedure, *Security of electronic information*, IGDS No. 164.
7. This Procedure is effective as of the date of issue.

Scope

8. This Procedure applies to all ILO departments, external offices and projects.

Replacement

9. For reasons of security, compatibility and maintainability, all IT devices must be replaced at the end of their useful life as determined by the maximum period of warranty available for this type of equipment. This includes IT devices used by ILO staff, external collaborators, interns, vendors, constituents, consultants, as well as devices located in kiosks, cybercafés, training venues, etc.

10. The timely replacement of obsolete IT devices is coordinated by INFOTEC in collaboration with the departments, external offices and projects. Existing IT devices are reviewed every six months for potential replacement.
11. Managers of departments, external offices and projects are responsible for ensuring sufficient funds are allocated to replace IT devices at the end of their useful life. For PCs (desktops and laptops) purchased before April 2020, the useful life is determined as four years. Devices purchased after April 2020 and installed with a standard ILO Windows 10 image have a useful life of five years. IT devices older than the useful life must imperatively be replaced within six months. An IT device that has not been replaced by the end of this six-month grace period will no longer be considered compliant with IT security and equipment standards and will not be able to access ILO systems. If an IT device is no longer able to access the ILO systems, managers are responsible to provide a compliant device so staff can continue to carry out their work without disruption.
12. A list of IT device hardware and associated software which are no longer supported and must be replaced can be found at: [IT equipment no longer supported](#).

Funding of purchase/replacement of PCs and laptops

13. The replacement of PCs for staff on regular budget (RB) positions is financed through a centralized PC purchasing allocation managed by INFOTEC. This allocation fully covers the cost of purchasing or replacing one standard ILO laptop, lock and docking station for every ILO staff member on an RB Core post once every five years.
14. Staff funded on RB Temp posts at headquarters will be provided with a laptop for the duration of their contract. These laptops must be returned to INFOTEC for re-assignment at the end of the RB Temp funded contract.
15. The centralized PC purchasing allocation can also be used to provide one additional laptop and docking station for field offices that have more than 25 RB funded staff, and two additional laptops and docking stations for field offices of more than 50 RB funded staff. These laptops should be used for staff on RB temp funded posts. They should be replaced every five years. Any additional requirements for laptops should be fully funded by the local office.
16. The decision to standardize on laptops rather than desktops is directly related to lessons learned during the extensive teleworking period experienced during the COVID-19 pandemic. Staff who had access to an ILO laptop with VPN access found it more reliable when working from home, than those who were obliged to rely on their personal devices.
17. Staff who have been provided with a managed ILO laptop are expected to use this laptop for accessing ILO systems at home, on mission or in the workplace. This ensures that ILO systems are kept secure and not inadvertently compromised through inadequately protected personal devices.
18. The funding of screens, keyboards and mice to be used with the laptop is the responsibility of the staff member's department or office.
19. Information regarding centralized purchasing of PCs can be found at: [Centralized purchasing of computers](#).
20. The current standards for ILO PCs and laptops can be found at: [Standards for official ILO computers](#).

21. For all users of PCs and laptops (with docking stations) who are not on an RB Core post (e.g. staff funded by Development Cooperation), the cost of PCs and laptops (with docking stations) must be fully borne by the department, external office or project.

Staff movement

22. Ad-hoc requests for replacing an existing desktop PC with a laptop and docking station before the end of its useful life should be made using the form: [Request for a laptop with docking station](#). Requesting units will be expected to fund such replacements from their own budget. For RB posts, a difference in cost between a laptop and a desktop must be funded; for extrabudgetary (EB) posts the full cost of the laptop with a docking station must be funded by the requesting unit.
23. Ad-hoc requests for replacing an existing laptop before the end of its useful life should be made using the form: [Request for a laptop with docking station](#). In such cases, the full cost of the laptop and new docking station (if needed) must be funded by the requesting unit.
24. When a headquarters user of any IT device moves to a new headquarters department, the user should open a ticket at the Service Desk to request that their devices be assigned to the new department and that the associated docking station be moved to the new office.
25. Any laptops that are unassigned as a result of a staff member departure, or move from one department or office to another, must be returned to the Service Desk (in headquarters) or the IT focal point (in the Regions) for re-assignment.
26. Staff who move duty stations are not allowed to take their IT device with them. IT equipment should remain in the location where it is inventoried.
27. PCs and laptops can only be reassigned to another user if they are less than their useful age (four years if purchased before April 2020; five years if purchased after April 2020). Smartphones or tablets can be reassigned if they are less than three years of age.

Request for additional or specialized equipment

28. INFOTEC's centralized PC purchasing allocation covers replacement of standard hardware models and configurations. Any request for additional or specialized equipment, such as an oversized monitor, ergonomic keyboard, extra memory, wireless mouse, etc., requires the approval of the director/responsible chief of the department or external office and is subject to technical clearance by INFOTEC.
29. Any request for additional or specialized equipment must be funded by the department, external office or the ILO's accommodation fund where applicable.
30. For headquarters staff, the form to request additional or specialized equipment can be found at: [Request for specialized equipment](#). Staff in the Regions should contact their IT focal point.

Laptop loans

31. Headquarters staff members who need to undertake official travel or who telework occasionally and whose desktop PC has not yet been replaced by an ILO laptop, can request the temporary use of a stand-alone laptop from INFOTEC. INFOTEC maintains a pool of laptops and prepares laptops for loan on demand. The patching of stand-alone laptops is managed by INFOTEC to ensure that they are appropriately secured. INFOTEC also ensures that the most recent ILO standard software is installed and ready for use by the staff member.
32. Requests for an INFOTEC laptop on loan must be sent to the INFOTEC Service Desk (servicedesk@ilo.org) at least three working days in advance of travel or teleworking to ensure sufficient time is allocated to prepare the laptop. INFOTEC cannot always guarantee that a laptop will be available, particularly if this notice period is not observed.
33. The form to request a laptop on loan at headquarters can be found at: [Request for laptop loan](#).
34. Where applicable, staff in external offices should address their loan requests for stand-alone laptops to their IT focal point.

Smartphones and tablets

35. ILO standard smartphones and tablets may be provided to an ILO staff member with a demonstrated business need.
36. ILO smartphones will be installed and managed through the ILO's mobile device management system. This system is designed to ensure that ILO data accessed through the smartphone is protected from theft or accidental loss.
37. Requests for provision of an ILO standard smartphone or tablet must be approved by the staff member's responsible chief. Costs associated with the purchase or replacement of a smartphone or tablet are the responsibility of the staff member's department, external office or project.
38. The form to request an ILO smartphone for a staff member at headquarters can be found at: [Request for headquarters ILO smartphone](#).
39. The form to request an ILO tablet for a staff member at headquarters can be found at: [Request for headquarters ILO tablet](#).
40. Monthly subscription fees associated with ILO mobile data and telephony plans are the responsibility of the staff member's department, external office or project. ILO tablets are not configured with a SIM card and can only be used with a Wi-Fi connection. No subscription fees are associated with ILO tablets.
41. For more information about current data and telephony plans at headquarters, please refer to: [ILO headquarters mobile data subscription plans](#).
42. In external offices, IT focal points should be consulted on the process to purchase smartphones and tablets as subscription plans vary. Where economically viable, external offices should purchase the same brands and models of smartphones and tablets prescribed by INFOTEC.
43. Staff members issued an ILO smartphone are requested to limit their data usage. Given the large quantity of media available over the web, it is very easy for an ILO staff member to exceed the limits of the data plan that has been negotiated by the Organization with a local service provider. In order to reduce data usage, the staff member concerned should note that streaming music, downloading or watching videos, interacting with social networks and other applications running in the background on the smartphone should be avoided until the staff

member is connected to a Wi-Fi network. Using these services over a cellular network, especially when roaming outside of the covered service area, may result in increased monthly subscription costs and must be avoided. In this context, roaming should be turned "off" as well as mobile data for such applications.

44. Recommendations on how to cut down on mobile data usage can be found at: [Tips on lowering mobile data usage](#).
45. ILO issued SIM cards must not be removed from ILO issued/loaned smartphones or cell phones and placed into personal devices. Staff members who remove the ILO issued SIM from the official phone and place it in their personal device are responsible for covering any charges incurred while using the ILO SIM.
46. If an ILO smartphone or a tablet issued by headquarters is damaged, the requesting department or external office is responsible to arrange for repairs and cover the cost to repair or replace the device. More information about the repair and replacement of damaged smartphones and tablets can be found at: [Repair or replacement of smartphones](#) and tablets.
47. Charges related to personal use of smartphones are not covered by the ILO's mobile subscription plans and must be declared by each staff member. Personal charges declared by staff who received an official mobile phone in headquarters will be automatically recovered from staff members through payroll. External offices should follow their existing cost recovery procedures.
48. In the event a staff member is retiring, and their ILO smartphone or tablet is older than three years, the respective department or external office can opt to donate the device to the future retiree. The procedure to follow when an obsolete ILO tablet or smartphone is retained by a future retiree is described in more detail here: [Keeping your ILO smartphone or tablet upon retirement](#). This procedure must be completed by the staff member before leaving the organization.

Required training

49. Successful completion of the ILO's Information Security Awareness Programme is mandatory for all users of IT devices. A grace period will be provided for users to complete the training. If training is not completed by the end of the grace period, access to ILO systems will be restricted. Instructions on how to access the Information Security Awareness Programme can be found on the INFOTEC Intranet.
50. Staff who are to be issued a smartphone, tablet or laptop (including those available on loan) must have completed the ILO's Information Security Awareness Programme prior to receiving the device. INFOTEC will only issue a new laptop or a smartphone to staff after receiving confirmation that they have completed this training.

Cell phone loans

51. Headquarters staff members on mission may request the loan of an ILO cell phone. These phones have limited data capabilities (e.g. internet use) and are primarily used for making phone calls. Charges will only be applied to the staff member's department or external office during the period of the loan. Costs associated with personal calls on ILO cell phones must be declared by staff members.
52. The form to request an ILO cell phone at headquarters for loan for a mission can be found at: [Request for headquarters ILO cell phone](#).

53. For more information about current mobile data and telephony plans at headquarters, please refer to: [ILO headquarters mobile data subscription plans](#).

Bring user's own device

54. With respect to personally owned devices used to access the ILO systems, the user must comply with all relevant ILO directives and procedures as well as the ILO IT security policy.

Software licences

55. INFOTEC procures licences for all standard software deployed across the ILO. Software licences are required on every PC or laptop that connects to the ILO's network.
56. INFOTEC is responsible for the installation of official ILO software on IT devices.
57. ILO software is the property of the Office and must not be installed on equipment that does not belong to the ILO.
58. Many vendors charge for software licences per device. This means that a staff member using two computing devices (i.e. a laptop at home and a second laptop or a PC in the Office) would require two sets of software licences. For this reason, the Office has decided that staff can be provided with either a laptop and docking station, or a PC, but not both. From April 2020, staff will be provided with a single laptop and docking station. Any exceptions to this decision must be justified and fully funded by the requesting department or office.
59. Some departments or external offices may require non-ILO standard software in order to carry out specialized work. Requests for non-ILO standard software at headquarters must be sent to the INFOTEC Service Desk (servicedesk@ilo.org) for technical assessment and approval prior to purchase. Requests from external offices should be routed through the local IT focal point to the IT Regional Administrator who will review the request and then send it to the INFOTEC Service Desk if applicable.
60. INFOTEC will evaluate all requests for specialized software to ensure there are no security implications or compatibility issues with other software being used by the Office. INFOTEC will also assess software deployment models and associated maintenance costs to ensure sustainability over the long term.
61. For all items that are physically purchased by INFOTEC, a record of installed licences will be maintained to ensure compliance with license purchase use. Under no circumstances will INFOTEC install more licences than have been purchased by the Office.
62. The form to request specialized (non-standard) software can be found at: [Request for specialized software](#).

Software maintenance

63. Regular patching and updating of operating systems and software is needed to address the risk of IT devices being exploited by malware or hacking attacks, potentially resulting in the loss of data, breach of ILO IT infrastructure, etc.
64. In addition to addressing security deficiencies, software updates also:
- optimize the use of the resources by the operating system;
 - add newer and more secure features;
 - remove old and unprotected features; and

- update device drivers to increase software efficiency.
65. The patching of standard PCs and laptops with docking stations is initiated automatically by INFOTEC when these devices are connected to the ILO network.
 66. Equipment that has not been patched for more than 90 days will be automatically prevented from accessing the ILO systems. The PCs or laptops should be returned to INFOTEC or the IT focal point for patching before network access is restored.
 67. Staff members using ILO smartphones and tablets must also connect to the internet (through Wi-Fi) frequently to download and apply the latest software patches.

Keeping data secure

68. Users should avoid keeping official ILO data on the C: or D: drive of their PC or laptop. These drives are not backed up by INFOTEC and in the event of a hardware failure, or loss of the device all data stored on these drives will be irretrievable. If these drives become encrypted as a result of a ransomware attack the data stored on them will also be lost.
69. If users choose to store personal data on their local C: or D: drives, it is their responsibility to back up this data up to a personal external hard drive, USB stick or cloud file storage solution.
70. Official ILO data that can be shared with colleagues should be stored on departmental file servers or the I: drive.
71. Official ILO data of a confidential nature should be stored on the G: drive.
72. Users should not store any personal data such as music, videos, photographs, financial documents, password files, copies of identity documents, etc. on departmental file servers, I: drive or G: drive as these network drives are backed up and retained for 10 years.

Lost or stolen equipment

73. If an IT device issued from headquarters is lost or stolen, the staff member must immediately notify the INFOTEC Service Desk (servicedesk@ilo.org) and the Information Security and Assurance Services Unit (isas@ilo.org). INFOTEC or IT support technicians shall seek to locate the device and/or remotely wipe the contents to prevent any data loss or security breach. Field staff must contact their IT focal point.

Disposal

74. INTSERV is responsible for maintaining an inventory of all IT devices. Asset details are linked to the department or external office concerned.
75. When equipment becomes obsolete or is donated, all data and software must be deleted prior to removing the device from the inventory.
76. For additional details concerning the disposal of electronic devices, please refer to Office Procedure, *Furniture and equipment*, IGDS No. 281.

77. The disposal process for PCs and laptops can be found at: [PC and laptop lifecycle](#).

Mark Mongillo
Director, INFOTEC