

INTOSAI DEVELOPMENT INITIATIVE

IT AND TECHNICAL EQUIPMENT
POLICY AND GUIDELINE

TABLE OF CONTENTS

VERSION DETAILS	2
A. Purpose & Scope	2
B. Description of IT Resources, Technology Related Assets and Services	3
C. Policy for Procurement of IT Assets and Services	3
General Provisions	3
Hardware	4
Software.....	4
Applicable: IDI Staff Services.....	4
D. Inventory of IT Assets	5
E. Usage of IT Assets and Services	5
General guidance	5
Laptop Usage	5
Network Usage.....	5
Mobile Phone Usage	6
Backup.....	6
F. Maintenance of IT Assets and Services	6
General.....	7
Business Continuity and Disaster Recovery	7
G. Security	7
Laptops.....	7
Network Security	7
Mobile Phone.....	8
H. Life Cycle and Disposal/Recycling of IT Assets	8

VERSION DETAILS

1.	Date Effective from	07 October 2024
2.	Process of Development and Approval	Erstwhile Information and Technology Policy for IDI and IDI Mobile Phone Rules have been subsumed into this policy. Approved by the IDI Director General in consultation with the members of the IDI management team after obtaining comments from IDI staff.
3.	Schedule of Maintenance	Version review in 2027
4.	Version being replaced	This policy replaces the Information and Technology Policy for IDI and IDI Mobile Phone Rules
5.	Available at	www.idi.no

A. Purpose & Scope

Purpose

This policy details the guiding principles related to Information Technology (IT) assets and services of IDI.

Scope

- The policy and guidelines shall be applicable to the IDI Administration, all IDI staff and those working on behalf of IDI at all times of handling IT and related assets and services including beyond office hours and on holidays.
- This policy should be read in conjunction with all other IDI policies.
- It covers the procurement, inventory, usage, maintenance, and disposal and security of IT and related assets and services.
- It also covers the procurement and use of technical equipment, or services provided by IDI to staff for facilitating their work within and outside office premises. Eg. Mobile phone, equipment for home office, internet subscription at home.
- **Policy statements have been numbered in the policy and the supporting guidelines for the respective policy statements, wherever applicable have been indicated in boxes.**

B. Description of IT Resources, Technology Related Assets and Services

In IDI's context, IT and related assets include hardware, software and services:

- Hardware such as laptops, monitors, printers, video conferencing equipment and cameras, data storage devices, any other device provided by IDI.
- Software like operating systems, purchased application software, software subscriptions, mobile phone apps for official use etc.
- Services including Managed Services, Software as a service - SaaS (i.e. O365 including MS Teams and Outlook), Platform as a Service - PaaS (i.e. Xledger, LMS), Infrastructure as a Service IaaS (some IT infrastructural support from the service provider), workspace solutions messaging and meeting solutions, email service, website hosting and maintenance, cloud storage solutions.

C. Policy for Procurement of IT Assets and Services

General Provisions

1. Administration or Staff can procure IT Assets by direct purchase or through leasing.
2. All regulations in the IDI Procurement policy or in this policy shall apply for both direct purchases and lease agreements
3. Administration shall facilitate the procurement of a mobile phone for staff. Procurement may be made directly after approval by Administration and reimbursement can be obtained. The configuration and capacity of the mobile phone will follow the IDI guideline to meet the operational need.
4. Staff are entitled to receive a taxable refund from Administration for internet connection for home office.
5. Staff may purchase devices such Monitor, Keyboard & Mouse set, etc. for home office and get reimbursed by Administration as per IDI Policy.
6. Administration must endorse the capacity/ capability/ configuration of any IT asset that is to be procured. IDI Administration must consider necessary aspects such as user requirements within IDI, implementation, support and maintenance, upgrades (for applicable cases), usage risks if any, built in security features and warranty conditions.
7. Staff and Administration must undertake a cost benefit analysis and consider the risk of obsolescence while procuring an IT asset and its available version. The analysis should also inform a purchase vs leasing decision.

➤ Latest versions are typically substantially higher in cost as compared to mid-life versions of the asset. Versions nearing end of life will typically run out of Original Equipment Manufacturer (OEM) support.

Hardware

- Laptops are currently leased through IDI's IT partner
- Monitors, printers, video conferencing equipment, cameras, etc. are purchased or leased.

Software

- System software typically instructs the computer to do something. It controls the operational and processing functions of the computer. E.g. Microsoft Windows managed and installed by IDI's IT Partner in laptops and iOS or android for smart phones.
 - Application Software and Apps are designed to perform specific functions or a group of closely related functions. Apps are more common in the context of mobile phones) being procured should be compatible for integration with other existing software in use in IDI. To ensure this, software should be procured in consultation with Administration.
8. Staff shall procure any software in consultation with Administration for ensuring compatibility of integration with existing software/
 9. Staff shall take approval from Administration to install any specific software in the laptop. Any accidental installation of malicious software should be reported immediately to IDI Administration.

Applicable: Staff Services

10. Administration shall evaluate the requirement for outsourcing or procuring specific IT and related services based on the needs of the users within the organization.
 - Services shall be distinguished between those that are to be used at the organisation level including workspace solutions, website hosting etc. and those that are used at individual level including internet connectivity (at residence), mobile subscriptions etc. Individual level services are not covered in this policy.
11. Administration will be responsible for procuring the appropriate services at the organization level fulfilling the necessary utility and value for money considerations. Interoperability in terms of cohesive communication across different IT platforms, equipment and other services shall be ensured.
 - For services being paid/ reimbursed to individuals by the IDI, IDI Administration shall retain the right to ensure due diligence checks and utility and value for money considerations. This might include among others, a check of the bill details for the service.

D. Inventory of IT Assets

➤ Hardware like laptops are leased but other assets are purchased. Such purchased assets are expensed upon procurement and not capitalised or depreciated. Software is expensed over the period of their usage.

12. Irrespective of capitalisation of assets, Administration shall maintain and update an inventory/ inventory register of all IT and related assets. These shall include hardware including laptops, mobile phones, printers, cameras, etc. All IT asset purchases made by IDI work streams should be reported to IDI Administration immediately.
13. Administration will review annually the Inventory register to ensure its completeness and to evaluate use of different software, hardware and licenses.

E. Usage of IT Assets and Services

General guidance

14. All hardware, including laptops and mobile phones procured by IDI and issued to IDI staff shall remain the property of IDI at all time.
15. All IDI Staff shall work through and use the workspace solutions provided by IDI.

➤ All IDI staff are expected to be conversant with use of basic IT hardware, software and services. Basic familiarisation with IDI IT systems will be provided by IDI Administration to all new IDI staff as part of their induction.

➤ The need for any specific training shall be communicated by the concerned IDI staff to their manager and IDI Administration.
16. Under no circumstances should IDI laptop be used to engage in proscribed/ prohibited or unethical/ illegal activities.

Laptop Usage

17. Administration will provide one pre-configured laptop to each staff with the necessary operating system and software packages. The need for an additional laptop for operational purposes shall be approved by the relevant department head and communicated to IDI Administration.

Network Usage

➤ Within IDI premises, all staff laptops and office printers will be connected to the Local Area Network and common internet.

Mobile Phone Usage

- staff shall have the mobile contract that is the most economical for IDI given their usage pattern. IDI will cover the following:
 - Oslo based staff have a subscription with up to 20 GB data, free calls and text messaging in Norway/EEA and "SafeZone" for mobile security to protect against unsafe websites.
 - All Staff have a maximum of NOK 12000 per annum of all use abroad with their mobile phone.
 - For staff who are not on the 20 GB plan it is possible for employees to purchase more data.
 - It is possible to purchase data package for use abroad using the service provider's app
 - IDI staff based outside Norway get a fixed mobile monthly allowance or included in the salary
- Costs not covered that will be withdrawn monthly from salary:
 - Mobile content services and payments via mobile phone for goods / services.
 - Information Service (1880 1881, 1888 etc.). MBN app or internet search engine should be used instead of calling 1881.
 - Telephone numbers starting with 800, 810, 815-, 820-, 829- and 5-digit numbers.
 - Data usage and calls beyond the subscription.
- Staff are provided with a protective back case and glass covering that must remain on the mobile phone at all times.
- Monitoring of mobile costs are "outsourced" by IDI. The outsourced company will send a link each month to anyone who has a cell phone plan, with information on costs and use in the month before and specification of what would be from next month salary.
- The mobile phone can be used during paid leave, unless otherwise agreed between manager and employee.
- Upon retirement or termination of employee contract the mobile phone shall be returned to IDI or purchased at a fair market rate.
- Mobile use outside Norway: Mobile use abroad can be very costly, especially the use of mobile data. It is therefore expected that IDI employees are responsible and hold private use at a minimum level. Less expensive alternatives should always be used when available.

Backup

18. Staff shall be responsible for backing up all their work in the workspace solutions (currently O365 Teams and SharePoint which provide for automatic back up) as made available to them by IDI Administration. IDI staff need to ensure that all resources prepared/ handled by them as part of their IDI work should be easily accessible to their colleagues, by saving them at the appropriate location in the workspace solution.
19. In case of confidential information, location in Teams/ Sharepoint needs to be shared by the staff member with the concerned Head of Department or Head of Administration.
20. New MS Team can be created by staff with approval from Administration through the Overview & Control App.
21. All documents pertaining to old Strategic Plan periods (i.e. ones preceding the immediately prior one) are archived and stored by IDI Administration.

F. Maintenance of IT Assets and Services

General

- Maintenance of IT assets and services includes all aspects like managing uptime, providing trouble shooting services, saving and archiving data and information, ensuring business continuity in IDI and disaster recovery.
 - IT assets and services of IDI are managed by different managed service partners appointed by IDI. These include workspace solutions, maintenance of hardware like laptops and printers etc., website maintenance etc.
22. IDI Administration is responsible, through IT Partner, Designated managed service provider as necessary, to ensure availability of necessary services, performance, and continuous improvement of the IT assets and services (i.e., operation of software and hardware).
23. IDI Administration will be responsible for timely resolution of reported incidents or problems.
24. IDI staff shall report any incident or problem related to IT directly to IT partner and IDI Administration.

Business Continuity and Disaster Recovery

25. IDI Administration will ensure suitable contractual provisions with managed service providers for ensuring business continuity and disaster recovery of IT hardware and systems including laptops, printers, workspace solutions like Microsoft 365, office network, website etc.
26. On an annual basis, IDI Administration shall obtain an assurance from the managed service providers regarding the functioning of the agreed business continuity and disaster recovery mechanisms.

G.Security

Laptops

Password

27. Staff must update the laptop password as necessary and based on the applicable rules. IDI's Active Directory must have an account locking policy after the prescribed number of failed attempts.
- Access to Staff Laptops: Staff access to a laptop will set as regular / restricted user (e.g., No Administrator privilege), to avoid any unauthorized version of software installation which may lead to security threat. Administration privileges can be provided to Staff for necessary operational need for a specific duration.
 - Software scan: IDI will ensure periodic scan on IT Assets (e.g., Staff laptop) to identify potential malware software developed by cybercriminals often called hackers. Any new software must go through relevant security scanning prior to launching in IDI environment.

Network Security

- Network security is enabled in all PCs through Firewall, Web Security and Email Security software.

Anti-virus

28. To ensure security of information IDI Administration will ensure necessary antivirus / malware protection for laptops and network.

Mobile Phone

29. Staff's mobile phone must follow a 6 digits pin for authentication and needs to follow IDI's active directory policy (e.g., lock account after x no of fail attempt). It is not allowed to remove the SIM PIN

- It is not permitted to download and / or forward programs or documents that are flagged as dangerous by the mobile phone security system
- Available anti-theft mechanisms on the mobile phones should be kept activated
- In case of loss of the phone, the phone and SIM card should be locked immediately.

H. Life Cycle and Disposal/Recycling of IT Assets

Life Cycle

30. Mobile phones and Laptops, have a normal life cycle of 3-5 years. For environmental reasons replacement will be done when laptops/mobiles no longer work properly. IDI staff requiring replacement of laptops shall return old devices to IDI administration.

- Network printers and scanners will be replaced when they are no longer working properly.
- Any exception of hardware lifecycle can be approved by DDG Administration. End of lifecycle assets will follow the guideline mentioned in disposal section.
- When repair cost is too high after looking at the current value (taking depreciation into account), and the age of the equipment, the hardware/ peripheral will be written off.

Disposal/Recycling

31. IDI Staff and Administration must ensure necessary archiving and removal of data, software, documents, etc. from the asset before sending to recycling. This applies also to devices that Staff can keep for personal use.

- Electronics contain both toxic and highly valuable materials which must be handled properly. After completing their lifecycle, all IT assets must be recycled via OAGN, IT Partner or Leasing Agency.