ISO/IEC 27001:2022(E)
Information Security Controls

https://www.iso.org/isoiec-27001-information-security.html

Control #	Control short title	Organizational control	Relevance to Telecoms and mobile ICT
5.7	Threat intelligence	*Information relating to information security threats shall be collected*	Security threats on mobile devices can take the form of apps which collect data, web pages that collect or monitor data, as well as text-based phishing threats.
5.9	Inventory of information and other assets	*An inventory of information and other associated assets, including owners, shall be developed and maintained*	Associated assets include the endpoint devices providing access to the information, as well as the related connectivity services. An inventory of device and connection assets msut be kept.
5.10	Acceptable use of information and other associated assets	*Rules for the acceptable use and procedures for handling information and other associated assets shall be indentifieed, documented and implemented*	This would need to include mobile use policies and remote working policies.
5.11	Return of assets	*Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.*	Employee offboarding almost always involves the retrieval of company endpoint equipment. This can only be done effectively if there is a maintained register ofr mobile device assets linked to employees.
6.7	Remote working	*Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises*	Securing connections may require encryption. Securing other WFH items may include home disks, home routers, personal Wi-Fi, as well as fixed cellular devices.
7.9	Security of assets off premises	*Off-site assets shall be protected.*	Stolen or lost mobile devices present not just a financial loss but also a security risk to companies.
7.10	Storage media	*Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.*	Mobile devices, including phones, can and do store sensitive information (contacts, notes, etc.), as well as possibly csutomer or staff PII. The full device lifecycle must be managed.
8.1	User end point devices	*Information stored on, processed by or accessible via user end point devices shall be protected*	This includes stored credentials, address book contacts, corporate apps, notes, photos, payment info, and more. User end point devices includes IOT devices.
8.7	Protection against malware	*Protection against malware shall be implemented and supported by appropriate user awareness*	Malware is as relevant to mobile endpoints as to fixed endpoints. Malware can be deployed via text phishing or via sideloaded apps. Mobile Threat Defence (MTD) required.
8.10	Information deletion	*Information stored in information systems, devices or in any other storage media shall be deleted when no longer required*	Mobile devices, including phones, can and do store senstive information (contacts, notes, etc.), as well as possibly csutomer or staff PII. Removing such data when no longer required mostly involves doing it remotely. This includes when a device may be lost or stolen.
8.15	Logging	*Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed*	It is reasonable that logs of events on mobile devices are part of this requirement. Mobile Threat Defence (MTD) is required to log specific "relevant events" such as a vulnerability or an attack.
8.19	Installation of software on operational systems	*Procedures and measures shall be implemented to securely manage software installation on operational systems*	Ensuring all software updates are applied to all mobile devices is a part of this.
8.21	Security of network services	*Security mechanisms, service levels and service requirements of network services shall be indentified, implemented and monitored*	A zero-trust model of authentication is required.
8.23	Web filtering	*Access to external websites shall be managed to reduce exposure to malicious content*	Globally, a majority of webpage fetches are done on mobile devices. Managing external website access is not effective unless applied to mobile devices too.

END OF DOCUMENT