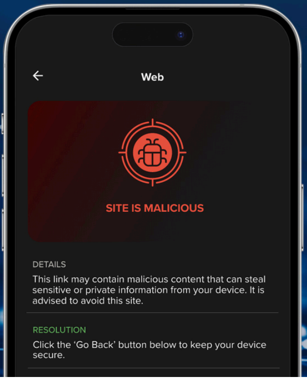
ZIMPERIUM®

# ISM Compliance for Mobile with Zimperium MTD



SITE IS MALICIOUS

DETAILS

This link may contain malicious content that can steal sensitive or private information from your device. It is advised to avoid this site.

RESOLUTION

Click the 'Go Back' button below to keep your device secure.

Zimperium has identified its "Top 10" ISM Mobile Controls. This mapping illustrates how Zimperium's Mobile Threat Defense (MTD) solution can support compliance efforts by summarising the control, the associated risks, and the corresponding compliance or mitigation strategies.

| Control | Summary | Risk? | Zimperium Sovereign-Hosted MTD |
|---|---|---|---|
| ISM-1088 | Personnel should promptly report potential compromises involving mobile devices, removable media, or credentials, including unusual device behaviour. | Exploited devices can directly lead to a mobile-led data breach and persistent compromise of Commonwealth information. | **Comply**<br>MTD detects and reports mobile attack events, with forensic data, to the department's security team. |
| ISM-1299 | When travelling, avoid connecting your mobile to public Wi-Fi, untrusted peripherals, chargers, or laptops. Scan for malware, ensure secure communication, use secure messaging and regularly reboot your device. | Mobile devices are vulnerable to attacks via cellular, Wi-Fi, and physical connections, potentially leading to data breaches and persistent spying. | **Comply**<br>MTD detects technical events, monitors for network and cable-based attacks, and suggests device reboots. |
| ISM-0240 | Paging, MMS, SMS and messaging apps are not used to communicate sensitive or classified data. | Mobile messaging apps like iMessage or Signal can be compromised by exploit vendors. Data sent via mobile apps is untrusted if the device is compromised. | **Comply**<br>Web Content Filtering can block unapproved services and app traffic by specific domain or category. |
| ISM-0863 | Mobile devices prevent personnel from installing non-approved apps once provisioned. | Non-approved apps may violate privacy or security policies. Over 70,000 unique mobile malware samples are discovered weekly by Zimperium. | **Mitigate**<br>MTD detects, vet and inform MDM of malicious or non-approved apps for removal. |

| Control | Summary | Risk? | Zimperium Sovereign-Hosted MTD |
|---|---|---|---|
| ISM-0864 | Mobile devices prevent personnel from disabling or modifying security functionality once provisioned. | Disabled security functions increase vulnerability to exploits, raising the risk of device compromise and a mobile-led data breach. | **Mitigate**<br>MTD detects system modifications and changes to security settings. |
| ISM-1300 | Upon returning from overseas travel, personnel must sanitise mobile devices and removable media, reset compromised credentials, and report and integrity failures. | Persistent exploits and malware attacks on Australian mobile devices while travelling can report back to foreign servers upon return. | **Mitigate**<br>MTD detects mobile compromise and integrity failures with forensics. |
| ISM-1366 | Security updates are applied to mobile devices as soon as they become available. | Mobile vulnerabilities are quickly weaponised by threat actors, leading to persistent spying, mobile-led data breaches, or lateral movement into an organisation. | **Mitigate**<br>Zimperium provides mobile Risk Based Vulnerability Management (RVBM), exploitability intel, and MDM integration for patching. |
| ISM-1555 | Before travelling abroad with mobile devices, record device details (product types, serial numbers, IMEI numbers), update operating systems and apps, remove non-essential data, apps, and accounts, and back up the device. | Compromised devices may return travel without being identified and processed correctly. Without a pre-travel backup, investigations are more difficult. | **Mitigate**<br>MTD identifies missing OS updates and vulnerable applications. |
| ISM-0869 | Mobile devices encrypt internal storage and removable media. | Without encryption, threat actors can easily extract information, leading to mobile-led data breach. | **Mitigate**<br>MTD detects if a device and its external storage are encrypted. |
| ISM-1888 | Mobile devices are configured with secure lock screens. | Without a device lock, threat actors can easily extract information from mobile devices and its apps leading to data breach. | **Mitigate**<br>MTD detects the removal of a device lock. |

ZIMPERIUM®

**Learn more at:** zimperium.com
**Contact us at:** 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244