RTLS INTELLIGENCE PTY LTD

MOBILE DURESS AND PERSONAL ALARM SYSTEMS STANDARD

DR AS/NZS 5765.1:2026

Mobile Duress and Personal Alarm Systems:

Wireless Personal Safety Systems: All Wireless and RTLS Technologies

Part 1: Product Requirements, Performance Criteria, and Conformity Testing

Document Status	**INDUSTRY CONSULTATION DRAFT**: Mobile Duress and Personal Alarm Systems Standard — Open for Public Submissions from Industry, Regulators, and Stakeholders in Australia and New Zealand
Prepared By	RTLS Intelligence Pty Ltd
Date	2026
Reference Standard	Informed by DIN VDE V 0825-1 (VDE V 0825-1):2025-10 and DIN VDE V 0825-11 (VDE V 0825-11):2023-02 (Germany), adapted and extended for Australian regulatory and market conditions. The German pre-standards are the most comprehensive published technical requirements for wireless personal emergency signal systems currently in existence internationally.
Designation	DR AS/NZS 5765.1:2026 — Proposed designation, subject to confirmation by Standards Australia and Standards New Zealand upon formal acceptance into the standards development work program.

Disclaimer: This standard has not been adopted or endorsed by Standards Australia or Standards New Zealand. The designation DR AS/NZS 5765.1:2026 is proposed and will be subject to confirmation upon acceptance into the formal standards development program. This draft is issued solely for the purpose of industry consultation.

Industry Consultation Notice

DR AS/NZS 5765.1:2026 — Mobile Duress Systems (MDS)

Document Status	Industry Consultation Draft 1 — issued for public comment. This standard has not been adopted as a formal AS/NZS Standard. It is released solely for the purpose of obtaining feedback from industry, regulatory bodies, and other stakeholders in Australia and New Zealand.
Prepared By	RTLS Intelligence Pty Ltd, Australia
Issue Date	April 2026
Submissions Close	**1 September 2026**
Anticipated Next Stage	Review of submissions: September–October 2026. Revised Draft 2 issued for targeted review: February 2027. Targeted review period: February–April 2027. Final document prepared for submission to Standards Australia and Standards New Zealand: August 2027.
Jurisdiction	Australia and New Zealand
Submit Feedback	**Online portal only** — register and submit comments section by section. Comments submitted by email or other means will not be accepted.

Invitation to Comment

RTLS Intelligence Pty Ltd invites written submissions from all interested parties in Australia and New Zealand on the requirements set out in this draft standard. The purpose of this consultation is to ensure that the standard, prior to formal submission to Standards Australia and Standards New Zealand, reflects the practical experience and technical knowledge of those who design, manufacture, supply, deploy, operate, and are protected by mobile duress and personal alarm systems.

Submissions are welcomed from:

- Manufacturers and importers of mobile duress devices and personal alarm systems
- System integrators, installers, and managed service providers
- Third-party monitoring centres operating in Australia or New Zealand
- Employers and responsible organisations deploying mobile duress systems in any occupational, clinical, residential, correctional, or personal safety context
- Organisations providing health, aged care, disability, correctional, or community services in Australia and New Zealand
- Worker representative bodies, unions, and health and safety representatives
- Regulatory bodies in Australia and New Zealand, including Safe Work Australia, State and Territory WHS regulators, the Therapeutic Goods Administration (TGA), the Australian Communications and Media Authority (ACMA), WorkSafe New Zealand, Medsafe, Radio Spectrum Management New Zealand (RSM), Te Whatu Ora, Whaikaha, the Accident Compensation Corporation (ACC), and the Health Quality and Safety Commission New Zealand (HQSC)
- Standards bodies, including Standards Australia and Standards New Zealand
- Academic and research institutions with expertise in occupational health and safety, assistive technology, or wireless communications

How to Submit

Submissions should be made through this online consultation portal. Register an account, complete your stakeholder profile, and then use the commenting system to provide feedback on each section. Respondents are encouraged to reference specific clause numbers where feedback relates to a particular requirement, and to identify any supporting evidence, test data, or operational experience that informs their comments.

Important: Only comments submitted through this online consultation portal will be accepted. Submissions sent by email, post, or any other means will not be considered.

Submissions may address any aspect of the draft standard, including but not limited to: the technical requirements and performance criteria; the scope and application of the standard; the adequacy of referenced Australian and New Zealand standards and legislation; the feasibility of compliance for products currently available in the market; and any requirements that submitters consider overly prescriptive, unclear, or missing.

Submissions received after 1 September 2026 may not be considered in the preparation of Draft 2.

New Zealand Stakeholders

This standard is a joint AS/NZS standard and is equally applicable to products supplied and deployed in New Zealand. New Zealand stakeholders are specifically encouraged to provide feedback on any requirements that may interact with New Zealand legislation, including the Health and Safety at Work Act 2015 (NZ), the Health and Disability Commissioner Act 1994 (NZ), the Privacy Act 2020 (NZ), and regulations administered by WorkSafe New Zealand and the Ministry of Health New Zealand. Any New Zealand-specific regulatory considerations identified through the consultation process will be incorporated into the revised draft.

Disclaimer

This standard is a consultation draft only. It does not represent a finalised or adopted standard and shall not be cited as such. The requirements contained herein are subject to change following the consultation process. RTLS Intelligence Pty Ltd makes no representations as to the completeness or accuracy of the draft and accepts no liability for reliance upon it.

Foreword

Background

Mobile duress devices and personal alarm systems are deployed across a wide range of occupational, clinical, residential, and personal safety contexts in Australia and New Zealand. Despite their safety-critical function, these devices are frequently the sole means by which a person in distress can summon emergency assistance, and no Australian standard currently exists that specifies minimum technical requirements for such devices.

The consequences of this absence have been demonstrable. Products have entered the Australian market claiming duress and alarm capabilities that, on testing, have been found to be unreliable in field conditions. Alarm transmissions have failed silently. Fall detection algorithms have missed the majority of test falls. Geolocation data has been absent from alarm records. Battery life under operational conditions has fallen well short of published specifications. Personal data has been transmitted and stored without encryption, and hosted outside Australia without disclosure. These deficiencies do not merely represent breaches of consumer expectations. In a safety-critical context, they represent direct risks to life.

The preparation of this standard was undertaken following a period of market analysis, product testing, and consultation with operators, monitoring centres, and end-user organisations in Australia. The intent is to establish a performance floor: a set of minimum requirements that any product claiming to function as a mobile duress system in Australia or New Zealand must demonstrably meet.

Preparation of this Standard

This draft standard was prepared by RTLS Intelligence Pty Ltd. The technical requirements set out herein draw on the framework established by the German pre-standards DIN VDE V 0825-1 (VDE V 0825-1):2025-10 and DIN VDE V 0825-11 (VDE V 0825-11):2023-02, which represent the most rigorously developed published requirements for wireless personal emergency signal systems currently in existence internationally. These German pre-standards were prepared by the national working group DKE/AK 713.0.4 under the German Commission for Electrical, Electronic and Information Technologies.

The requirements in this draft have been substantially revised from the German source documents to reflect: the Australian and New Zealand regulatory environments (including the Privacy Act 1988

(Cth), the Privacy Act 2020 (NZ), the Work Health and Safety Act 2011 (Cth), the Health and Safety at Work Act 2015 (NZ), ACMA radiocommunications requirements, and NZ Radio Spectrum Management requirements); the broader range of wireless technologies deployed in Australian and New Zealand environments, including LoRaWAN, satellite IoT, and RTLS technologies not addressed in the German standards; occupational conditions in both countries, including remote and rural work environments; and the specific failure modes identified through market analysis of products available in Australia and New Zealand.

Governance and Independence

This Industry Consultation Draft was prepared by RTLS Intelligence Pty Ltd, an Australian company that operates in the real-time location systems and personal safety technology sector. RTLS Intelligence Pty Ltd is therefore a participant in the market that this standard is intended to regulate.

RTLS Intelligence Pty Ltd acknowledges that the preparation of a draft standard by a single market participant carries a perceived risk of conflict of interest, regardless of the technical merits of the document or the good faith of the drafters. This risk is treated explicitly rather than implicitly. The following governance arrangements apply during the consultation period and beyond.

Disclosure of Commercial Interests

RTLS Intelligence Pty Ltd discloses the following commercial interests potentially affected by this standard: the company supplies real-time location system technology, personal safety devices, and monitoring integration services in the Australian market. This disclosure shall be updated and republished at each subsequent draft revision.

No clause in this draft has been written with the intent of disadvantaging any identified competitor or of creating commercial advantage for RTLS Intelligence Pty Ltd. Where any clause may be perceived to do so, RTLS Intelligence Pty Ltd invites specific submissions identifying the clause and the perceived effect, and will publish its response to each such submission alongside the revised draft.

Co-Sponsorship

Prior to formal submission to Standards Australia and Standards New Zealand, this draft will be co-sponsored by one or more of the following (to be confirmed):

- an Australian university research group with relevant expertise in occupational health and safety, assistive technology, or wireless communications;

- a peak industry body in the alarm monitoring, aged care, disability services, or worker safety sectors;
- a non-competing operator or end-user organisation in a relevant deployment context.

Co-sponsors will participate in the review of public submissions, the preparation of revised drafts, and the formal submission to Standards Australia and Standards New Zealand. The names and roles of confirmed co-sponsors will be published in the next draft revision.

Independent Technical Review

Following close of public submissions on 1 September 2026, all submissions will be reviewed by an independent panel comprising at minimum:

- one representative from a NATA-accredited or IANZ-accredited testing laboratory with relevant scope;
- one representative from a tertiary research institution with relevant subject-matter expertise;
- one representative from an end-user sector (aged care, disability, healthcare, or worker safety);
- one representative nominated by a relevant regulatory body or worker representative organisation.

The composition of the panel will be published before submissions close. RTLS Intelligence Pty Ltd will participate in panel deliberations as the drafting party but will not chair the panel and will not have a determinative vote on any contested clause.

Submissions Handling

All public submissions received during the consultation period will be:

- logged with a unique submission identifier and the submitter's identity (subject to any request for confidentiality);
- classified by clause, by submission type (technical, regulatory, scope, drafting, governance), and by recommendation;
- published in summary form, with the response of the drafting party and any decision of the independent technical review panel;
- retained for inspection by Standards Australia and Standards New Zealand at the time of formal submission.

Confidential submissions will be accepted where a submitter identifies legitimate commercial-in-confidence content. Confidentiality applies to the submitter's identity and any commercial detail; it does not apply to the technical or regulatory substance of the submission, which will be addressed in summary form.

Standards Australia / Standards New Zealand Pathway

RTLS Intelligence Pty Ltd does not assume that this draft will be adopted by Standards Australia or Standards New Zealand. The submission to Standards Australia under the New Standards Project (NSP) process, and concurrently to Standards New Zealand, will include the full record of submissions, the independent panel's assessment, and the co-sponsors' positions. Standards Australia and Standards New Zealand will determine the appropriate technical committee, the scope of any approved project, and the further drafting and balloting process. The final standard, if adopted, may differ in substantial respects from this draft.

Intended Submissions

This standard is intended to be submitted to the following bodies for consideration:

- Standards Australia and Standards New Zealand, for development as a formal joint AS/NZS standard through the relevant technical committee
- Therapeutic Goods Administration (TGA), noting that certain MDS products may attract classification as medical devices under the Therapeutic Goods Act 1989 (Cth)
- Safe Work Australia, for consideration as a supporting technical reference for guidance on mobile duress systems across all workplace deployment contexts
- Australian Communications and Media Authority (ACMA), in respect of radiocommunications device compliance requirements
- State and Territory WHS regulators, noting that each jurisdiction administers its own WHS legislation substantially based on the Model WHS Act
- WorkSafe New Zealand, for consideration as a supporting reference for workplace health and safety guidance under the Health and Safety at Work Act 2015 (NZ)
- Radio Spectrum Management New Zealand (RSM), in respect of radiocommunications compliance under the Radiocommunications Act 1989 (NZ)
- Office of the Privacy Commissioner New Zealand, for alignment with the Privacy Act 2020 (NZ) and Information Privacy Principles
- Medsafe, for medical device regulatory considerations under the Therapeutic Products Act 2023 (NZ)

Feedback

This is the Industry Consultation Draft, Version 1.0, of this standard. Submissions are open to all interested parties in Australia and New Zealand. The submissions period closes 1 September 2026. RTLS Intelligence Pty Ltd invites written feedback from manufacturers, importers, responsible organisations, monitoring centre operators, healthcare and aged care providers, unions and worker representative bodies, regulatory agencies in both countries, and any other interested party. Submissions should be made through this online consultation portal. **Only comments submitted through the online portal will be accepted — submissions by email, post, or other means will not be considered.**

Amendments from Previous Editions

This is the first edition of this standard. There are no previous editions.

Version	Date	Summary of Changes
1.0	April 2026	Industry Consultation Draft 1. Issued for public comment by industry, regulatory bodies, and stakeholders in Australia and New Zealand. Submissions close 1 September 2026.

1 Scope

This standard specifies the minimum requirements for mobile duress devices and personal alarm systems (hereafter referred to as Mobile Duress Systems or MDS) that use any wireless communications network or real-time location system (RTLS) technology, including but not limited to public telecommunications networks, private wireless networks, and dedicated positioning networks operated in Australia and New Zealand.

This standard defines requirements for:

- System design and architecture
- Device functionality and alarm types
- Performance and response time criteria
- Positioning and geolocation capability
- Environmental and mechanical durability
- Electrical safety and radio frequency emissions
- Battery performance and lifecycle
- Pre-deployment testing and commissioning
- Alarm notification and escalation
- User information and documentation
- Conformity assessment and testing

The standard applies to MDS devices operating over any of the following wireless network and RTLS technologies:

- **Cellular networks:** 4G LTE, 4G LTE-M (LTE Cat-M1), NB-IoT (Narrowband IoT), 5G NR (New Radio), 5G RedCap (Reduced Capability)
- **Wi-Fi (IEEE 802.11 series):** Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), Wi-Fi 6/6E (802.11ax), Wi-Fi HaLow (802.11ah, sub-1GHz long range)
- **Bluetooth and BLE:** Bluetooth 4.x, Bluetooth 5.x, Bluetooth Mesh, BLE Beacons (iBeacon, Eddystone), BLE 5.1 Direction Finding with Angle of Arrival (AoA) for sub-metre indoor positioning
- **Ultra-Wideband (UWB):** IEEE 802.15.4z, FiRa Consortium UWB. Provides high-precision indoor positioning with sub-30cm accuracy.

- **Zigbee / IEEE 802.15.4:** Zigbee 3.0, Thread. Low-power mesh networks used in building and facility deployments.
- **Z-Wave:** sub-GHz mesh protocol used in building automation and aged care environments
- **LoRaWAN:** LoRa physical layer over public or private LoRaWAN networks, including The Things Network (TTN) and operator-managed networks. Particularly applicable for large outdoor sites and environments where cellular coverage is limited or unavailable.
- **Sigfox:** ultra-narrowband low-power wide area network (where operational coverage exists in Australia)
- **DECT / DECT ULE:** used in clinical and aged care facility deployments
- **RFID:** passive UHF RFID (ISO/IEC 18000-63, EPC Gen2), active RFID at 433 MHz or 2.45 GHz. Used for zone-level location in any facility where infrastructure-based positioning is deployed.
- **Infrared (IR) positioning:** active IR badge systems used for room-level location detection in healthcare environments
- **Ultrasound/Ultrasonic positioning:** used in clinical RTLS deployments for sub-room precision
- **Private Land Mobile Radio (PLMR) / PTT over cellular (PoC):** mission-critical communications networks including TETRA, DMR, P25 (where used for duress transmission)
- **Satellite communications:** LEO satellite IoT networks including Iridium, Globalstar, Skylo, and 3GPP Non-Terrestrial Network (NTN). Applicable for any MDS deployment where terrestrial coverage is absent or unreliable.
- **Hybrid multi-technology devices:** devices that combine two or more of the above technologies for redundancy, with automatic fallback between network types

Where a device operates over a combination of network technologies, all applicable requirements of this standard shall apply to each active technology layer. The device shall meet the response time requirements in Table 1 regardless of which network technology is active at the time of alarm.

The purpose of a Mobile Duress System (MDS) is to enable any person who carries or wears a mobile duress device (the MDS Wearer, as defined in Clause 3.14) to summon assistance promptly in an emergency, through voluntary and automatic alarm mechanisms, and where applicable to establish a voice or data communication link. This standard applies to MDS products regardless of the context in which they are deployed.

This standard applies to:

- Mobile duress devices carried or worn by any MDS Wearer (as defined in Clause 3.14) in any deployment context
- Personal alarm devices deployed in any clinical, residential, or community safety context
- Fixed or semi-fixed personal emergency call systems using cellular or Wi-Fi networks
- Combined GPS tracking and alarm devices

This standard does not apply to:

- Fixed nurse call systems governed by AS 3811:1998
- Fire detection and alarm systems governed by the AS 1670 series or AS 2201 series
- Wearable medical devices classified as therapeutic goods where the primary function is physiological monitoring rather than personal duress

2 Normative References

The following documents are referenced normatively and are indispensable for the application of this standard. For dated references, only the cited edition applies. For undated references, the most recent edition applies.

Australian Standards

- ACMA Technical Standards applicable to the radio technology in use, as published on the Australian Communications and Media Authority website (acma.gov.au)
- AS/NZS 60529:2004 (IEC 60529:2001, MOD), *Degrees of protection provided by enclosures (IP Code)*
- AS/NZS 62368-1:2022 (IEC 62368-1:2020, MOD), *Audio/video, information and communication technology equipment — Part 1: Safety requirements*
- AS/NZS ISO 45001:2018, *Occupational health and safety management systems — Requirements with guidance for use*
- AS/NZS IEC 60068.2.14:2020, *Environmental testing — Part 2-14: Tests — Test N: Change of temperature*
- AS/NZS IEC 60068.2.31:2019, *Environmental testing — Part 2-31: Tests — Test Ec: Rough handling shocks*
- AS/NZS CISPR 32:2015, *Electromagnetic compatibility of multimedia equipment — Emission requirements*
- AS/NZS CISPR 35:2017, *Electromagnetic compatibility of multimedia equipment — Immunity requirements*
- AS 2201.1:2007, *Intruder alarm systems — Systems installed in client's premises*
- AS ISO/IEC 27001:2023, *Information technology — Information security management systems — Requirements*
- AS/NZS 62133.2:2021, *Safety requirements for portable sealed secondary lithium cells and batteries*

Australian Regulatory Instruments

- Radiocommunications Act 1992 (Cth)

- Radiocommunications (Compliance Labelling) (Devices) Instrument 2017 (ACMA)
- Radiocommunications (Low Interference Potential Devices) Class Licence 2015 (ACMA)
- Radiocommunications (Short Range Devices) Standards 2022 (ACMA)
- Telecommunications Act 1997 (Cth)
- Telecommunications (Consumer Protections and Service Standards) Act 1999 (Cth)
- Australian Communications and Media Authority Act 2005 (Cth)
- Electrical Equipment Safety System (EESS)
- Therapeutic Goods Act 1989 (Cth)
- Therapeutic Goods (Medical Devices) Regulations 2002 (Cth)
- TGA Guidance: Regulation of software, including Software as a Medical Device (SaMD), 2024
- TGA Guidance: Unique Device Identification (UDI), 2023
- Work Health and Safety Act 2011 (Cth) (Model WHS Act)
- Work Health and Safety Regulation 2017 (Cth) (Model WHS Regulation)
- Safe Work Australia, Code of Practice: Managing the Work Environment and Facilities (2022)
- Safe Work Australia, Guide: Working Alone or in Isolation (2022)
- Privacy Act 1988 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- Privacy and Other Legislation Amendment Act 2024 (Cth)
- Australian Privacy Principles (APPs), Schedule 1 to the Privacy Act 1988 (Cth)
- Office of the Australian Information Commissioner (OAIC), Guide to data analytics and the Australian Privacy Principles (2018)

New Zealand Regulatory Instruments

- Health and Safety at Work Act 2015 (NZ)
- Health and Safety at Work (General Risk and Workplace Management) Regulations 2016 (NZ)
- WorkSafe New Zealand, Good Practice Guidelines: Working Alone (current edition)
- Health and Disability Commissioner Act 1994 (NZ)
- Privacy Act 2020 (NZ)

- Radiocommunications Act 1989 (NZ)
- Radiocommunications Regulations 2001 (NZ)
- Radio Spectrum Management New Zealand (RSM), General User Radio Licence for Short Range Devices (current)
- Electricity Act 1992 (NZ) and Electrical (Safety) Regulations 2010 (NZ)
- Therapeutic Products Act 2023 (NZ) — note: commencement deferred
- Medsafe, Guidance: Classification of Medical Devices under the Medicines Act 1981 (NZ)
- Te Whatu Ora (Health New Zealand), Health and Disability Services Standards NZS 8134:2021
- Whaikaha, Ministry for Disabled People, New Zealand Disability Strategy 2016–2026
- Accident Compensation Corporation (ACC), New Zealand Injury Prevention Strategy

International Standards

- ISO 9001:2015, *Quality management systems — Requirements*
- IEC 62443 series, *Security for industrial automation and control systems*
- GSMA IoT Security Guidelines

NOTE: Where a current Australian standard equivalent to a referenced international standard does not yet exist, the international standard shall apply directly until a formal Australian adoption is in place.

3 Terms and Definitions

For the purposes of this standard, the following terms and definitions apply.

3.1 Mobile Duress System (MDS)

A system for triggering and transmitting voluntary and automatic personal alarms in emergency situations, carried or worn by any person for whom rapid access to emergency assistance is a safety requirement. An MDS consists of one or more Mobile Duress Devices (MDD) connected via any wireless communications network or real-time location system (RTLS) technology to a Monitoring and Response Platform (MRP). An MDS may be deployed in occupational, clinical, residential, community, or personal safety contexts.

3.2 Mobile Duress Device (MDD)

A device carried or worn by a person that, in an emergency, triggers a voluntary or automatic personal alarm in the Monitoring and Response Platform (MRP), and where applicable, establishes a voice or data communication link. An MDD may take the form of a dedicated wearable device, a pendant, a wristband, a belt clip device, a lanyard-worn tag, a smartphone application operating as an MDD, or any other form factor designed for personal carrying or wearing.

NOTE: Where an MDD takes the form of a software application running on a general-purpose smartphone or tablet, the hardware requirements of this standard apply to the host device where the manufacturer specifies a minimum compatible device, and do not apply where the application is designed to operate on any user-supplied device. All functional, performance, notification, and data requirements of this standard apply to software-only MDDs without exception.

3.3 Monitoring and Response Platform (MRP)

A software platform, application, or monitoring centre that receives, displays, logs, and processes emergency alarm signals from MDDs, enabling reliable and immediate initiation of an assistance response. The MRP may be operated by a third-party monitoring centre, an employer, or a carer.

3.4 Emergency Signal

A data signal transmitted by the MDD to the MRP that triggers a personal alarm, including the identity of the device, its last known location, alarm type, and timestamp.

3.5 Emergency Activation Button

A physical or capacitive control element on the MDD used to manually trigger a voluntary emergency alarm. The Emergency Activation Button shall be coloured red and shall be clearly distinguishable from all other controls.

3.6 Voluntary (Manual) Personal Alarm

A personal alarm triggered by the deliberate manual activation of the MDD by the wearer. Upon activation, the MRP shall generate a visual and acoustic alert and receive the device identity and last known location.

3.7 Automatic (Non-voluntary) Personal Alarm

A personal alarm triggered automatically by the MDD based on sensor data or inactivity detection, without deliberate manual activation by the wearer. The following automatic alarm types are defined:

3.7.1 Tilt / Position Alarm

Triggered when the MDD detects that the device has been tilted beyond a defined angle and this condition persists for a defined duration, indicating the wearer may have fallen.

3.7.2 Inactivity / No-Motion Alarm

Triggered when the MDD detects that the wearer has been motionless for a defined period, indicating potential incapacitation.

3.7.3 Check-In Failure / Time Alarm

Triggered when the wearer fails to perform a required periodic check-in (confirmation) within a predefined time window.

3.7.4 Device Separation / Loss Alarm

Triggered when the MDD detects it has been removed from or separated from the wearer for a defined period.

3.7.5 Panic / Escape Alarm

Triggered when the MDD detects sudden, rapid, or frantic movement patterns consistent with a panic or flight response, persisting for a defined duration.

3.7.6 Fall Detection Alarm

A separate alarm category explicitly defined in this standard. Triggered when the MDD detects an impact event consistent with a fall (rapid vertical deceleration), followed by continued inactivity or abnormal body position. Fall detection shall be evaluated as a distinct capability from Tilt/Position Alarm.

3.8 Pre-Alarm

An intermediate alert generated by the MDD prior to transmitting a full automatic personal alarm. The pre-alarm gives the wearer an opportunity to cancel the alarm if not in distress. The pre-alarm shall be clearly distinct (audible and/or haptic) on the device.

3.9 Technical Alarm

A system-generated alert indicating a fault in the MDS, including loss of network connectivity, low battery, device tamper detection, GPS failure, or failure of a scheduled self-test. Technical alarms shall be indicated on both the MDD and the MRP.

3.10 Response Time

The maximum permissible elapsed time, measured from the point of alarm trigger (manual activation or automatic detection condition), to the successful receipt and display of the alarm in the MRP.

3.11 Geolocation

The determination of the physical location of the MDD using any available positioning technology. Location data may be expressed as GPS/GNSS coordinates (latitude/longitude/altitude), indoor zone or room designation, or a combination thereof.

3.12 MDS Operation

The secured operating state in which a MDD is registered, monitored, and actively communicating with the MRP. MDS Operation status shall be visually displayed on the MDD at all times.

3.13 Lone Worker

A person who performs work activity in isolation from other workers, without close or direct supervision, and where assistance from another person would not be readily available in an emergency. This definition is consistent with Safe Work Australia guidance on working alone or in isolation, and with WorkSafe New Zealand guidance on the same subject. Lone workers are one category of MDS Wearer (see 3.14) but this standard is not limited to lone worker deployments.

3.14 MDS Wearer

Any person who carries or wears an MDD, regardless of their employment status, clinical status, or the context of deployment. An MDS Wearer may include, but is not limited to:

- Lone workers across any industry or occupation
- Healthcare, aged care, and disability support workers
- Residents of aged care facilities, retirement villages, and supported living environments
- People living independently at home who have a health condition, disability, or personal safety need
- Patients or service users in community health, mental health, drug and alcohol, or disability services
- Workers in any occupation who may be exposed to aggression, violence, or risk of assault
- Workers and students in field-based, remote, or isolated environments
- Persons subject to family and domestic violence, or others with a court-ordered or voluntary personal safety plan
- Custodial and correctional facility officers and staff
- Any other person for whom rapid access to emergency assistance is identified as a safety, clinical, or personal requirement

3.15 Responsible Organisation

The employer, principal contractor, facility operator, care provider, support coordinator, or other entity that deploys and operates an MDS for the protection of workers, residents, clients, or other MDS Wearers.

3.16 Authorised Personnel

Persons who have been granted explicit authority by the responsible organisation to configure, modify, commission, or decommission an MDD or MRP.

3.17 Operator

A person who monitors the MRP in real time and is responsible for acknowledging alarms and initiating or coordinating an emergency response.

3.18 Monitoring Centre

A facility, operated by a third party on behalf of one or more responsible organisations, that provides continuous or on-demand monitoring of MDS alarms and coordinates emergency response.

3.19 Commencement of MDS Operation

The act of a worker or wearer activating and registering an MDD with the MRP at the start of a working period or period of risk. Commencement of MDS Operation initiates the monitoring and self-test cycle.

4 Minimum Requirements for Mobile Duress Systems (MDS)

This section establishes the minimum requirements that a mobile duress system (MDS) shall meet in order to be considered compliant with this standard. These requirements represent the performance floor: the minimum level of functionality, reliability, and safety that any product marketed as a mobile duress system in Australia or New Zealand must demonstrably achieve.

Requirements are divided into three subsections: general system requirements (Section 4.1), which apply to the MDS as a complete end-to-end system; requirements specific to the mobile duress device (MDD) (Section 4.2), which address the hardware and software capabilities of the wearable or portable device; and requirements for the monitoring/receiving point (MRP) (Section 4.3), which address the platform or service that receives, processes, and acts upon alarms transmitted by the MDD.

All requirements in this section use the normative language defined in Section 1. Requirements expressed as "shall" are mandatory for conformity. Requirements expressed as "should" are recommended but not mandatory.

4.1 General System Requirements

4.1.1 Response Times

The response times specified in Table 1 apply to all MDS products supplied in Australia and New Zealand. Response times are specified by Network Class (refer Clause 4.1.1A) to reflect the physical constraints of the underlying wireless technology while maintaining the safety intent of this standard.

All response times are mandatory maximums for the applicable Network Class. A product that cannot meet the response time for its declared Network Class does not comply with this standard.

Alarm Type	Class A (Cellular / IP / RTLS)	Class B (LPWAN — LoRaWAN, Sigfox, NB-IoT)	Class C (Satellite IoT)
Voluntary (manual) personal alarm	≤ 5 seconds	≤ 45 seconds	≤ 90 seconds
Pre-alarm (prior to automatic alarm)	≤ 15 seconds	≤ 60 seconds	≤ 120 seconds
Automatic alarm — Tilt/ Position	≤ 90 seconds	≤ 120 seconds	≤ 180 seconds
Automatic alarm — Inactivity/No-Motion	≤ 90 seconds	≤ 120 seconds	≤ 180 seconds
Automatic alarm — Check-In Failure (Time)	≤ 30 minutes	≤ 45 minutes	≤ 60 minutes
Automatic alarm — Device Separation (Loss)	≤ 30 seconds	≤ 60 seconds	N/A (not required)
Automatic alarm — Panic/Escape	≤ 10 seconds	≤ 45 seconds	≤ 90 seconds
Fall Detection Alarm	≤ 30 seconds	≤ 60 seconds	≤ 120 seconds
Technical alarm (network loss, battery, fault)	≤ 10 minutes	≤ 30 minutes	≤ 60 minutes

Table 1 — Required Response Times by Network Class. All values are mandatory maximums for the declared Network Class.

4.1.1A Network Class Definitions

For the purposes of Table 1, Network Classes are defined as follows:

- **Class A — Cellular / IP / RTLS:** any MDD that transmits alarm data over a cellular data network (4G/5G), a Wi-Fi or Ethernet IP connection, or a real-time location system

(RTLS) with persistent bidirectional communication. Includes smartphone-based MDDs.

- **Class B — LPWAN:** any MDD that transmits alarm data over a Low-Power Wide-Area Network technology including LoRaWAN, Sigfox, or NB-IoT, where the physical layer imposes duty-cycle constraints, limited payload size, or non-persistent uplink scheduling.
- **Class C — Satellite IoT:** any MDD that transmits alarm data via a satellite IoT constellation (e.g. Globalstar, Iridium SBD, Swarm/SpaceX, OQ Technology, Kinéis), where transmission windows are constrained by orbital pass schedules and regulatory power limits.

Where an MDD supports multiple Network Classes (e.g. cellular with satellite fallback), the product shall be tested against the response time for each declared class independently. The product literature and MRP display shall clearly indicate which Network Class is active at any given time.

4.1.1B Deployment Suitability by Network Class

The responsible organisation shall ensure that the Network Class of the deployed MDD is appropriate to the deployment context and the risk profile of the MDS Wearer. The following guidance applies:

- Class A devices are suitable for all deployment contexts where cellular or IP coverage is available.
- Class B devices are suitable for deployments where the extended response times in Table 1 are acceptable given the risk profile, and where cellular coverage is unavailable or impractical. Class B devices shall not be deployed as the sole MDS in high-acuity contexts (e.g. domestic violence, custodial duress) where immediate alarm delivery is a safety requirement.
- Class C devices are suitable for remote and rural deployments beyond terrestrial network coverage. Class C devices shall not be deployed as the sole MDS in any context where the wearer faces an immediate physical threat requiring response within 90 seconds.

The deployment risk assessment (Annex E) shall document the Network Class selection rationale and confirm that the response times achievable by the selected class are adequate for the identified risks.

4.1.2 Device Identity in Alarm Transmission

The MRP shall display the identity of the triggering MDD, the alarm type, the timestamp, and the last known geolocation for every personal alarm and technical alarm received.

4.1.3 Geolocation in All Alarms

All alarm transmissions shall include the most recently acquired geolocation of the MDD, derived from the best available positioning technology at the time of the alarm. The alarm transmission shall include: the geographic coordinates (latitude, longitude, and altitude where available), the positioning technology used (e.g. GPS/GNSS, A-GPS, Wi-Fi, BLE, RTLS, cell tower), and an estimate of accuracy (in metres or zone/room designation).

Where the primary positioning method is unavailable, the system shall automatically fall back through available technologies in order of decreasing accuracy. The age of the location fix (time since last acquisition) shall be included in every alarm transmission. Cell tower triangulation alone does not satisfy the indoor positioning requirement (see Table 4).

4.1.3A Location Accuracy Tiers

The positioning technology used by an MDD is not prescribed. Any technology or combination of technologies that demonstrably meets the accuracy requirement for the applicable Tier (Table 4) is acceptable. Compliance is assessed by measured performance under the test conditions specified in Clause 6, not by technology selection.

Tier	Environment	Mandatory Minimum Accuracy	Acceptable Evidence
1	Outdoor — any MDS Wearer operating outdoors	≤ 5 metres (95th percentile, open sky conditions)	Demonstrated accuracy under test conditions (Clause 6). Cell tower triangulation alone does not satisfy this requirement due to insufficient accuracy.
2	Indoor general — standard indoor deployments	Room-level or named zone identification	Demonstrated ability to resolve the wearer's location to a named room, zone, or area of no greater than 50 m² under test conditions (Clause 6).
3	Indoor high-accuracy — correctional facilities, emergency departments, memory care and locked dementia units, acute mental health inpatient units, high-dependency aged care (where individual risk assessment identifies sub-metre positioning as necessary)	Sub-metre: ≤ 1 metre (95th percentile)	Demonstrated ≤ 1 m accuracy under test conditions (Clause 6). The technology used is not prescribed; any technology achieving this accuracy in the deployed environment is compliant.
4	Remote / no-coverage — terrestrial coverage absent or unreliable	GPS/GNSS coordinates at time of alarm; if unavailable, last known fix with timestamp and age of fix	Demonstrated GPS/GNSS acquisition under open-sky conditions. Where satellite IoT is the transmission path, the alarm payload shall include the most recent GPS fix.

Table 4 — Location Accuracy Tiers. Compliance is assessed by measured performance, not by technology selection.

4.1.4 Continuous Network Monitoring

The MDD shall continuously monitor the availability of its primary and secondary wireless communications network(s). Loss of network coverage on the primary network shall be indicated visually and audibly on the MDD within 60 seconds. Where a secondary or fallback network is available, the MDD shall automatically switch to the fallback network.

4.1.5 Alarm Retransmission Until Acknowledged

Following transmission of a personal alarm, the MDD shall continue to retransmit the alarm at intervals not exceeding 60 seconds until a receipt acknowledgment is received from the MRP.

4.1.6 Alarm Log and Timestamp Display in MRP

The trigger time and acknowledgment time of every alarm shall be recorded and displayed within the MRP. Logs shall be retained for a minimum of 12 months.

4.1.7 Scheduled Self-Test

The MDS shall include an automated monitoring function that tests the communication path between MDD and MRP at intervals not exceeding 24 hours. A failed self-test shall result in the device being flagged as not operationally ready.

4.1.8 Registration and Deregistration

At the commencement and end of each MDS operating session, the MDD shall register and deregister with the MRP. This event shall be logged and displayed in the MRP.

4.1.9 Prevention of Accidental Power-Off

For dedicated hardware MDDs, manual switching off of the MDD shall be technically prevented during active MDS Operation, unless confirmed by a secure deregistration sequence.

For software-only MDDs operating on general-purpose smartphones or tablets (refer Clause 3.2, NOTE), the following requirements apply in lieu of hardware power-off prevention:

- the MDD application shall implement a persistent foreground service or equivalent operating-system mechanism that resists accidental closure by the user;

- the MDD application shall generate a technical alarm to the MRP if the application is force-closed, the host device is powered off, or the operating system terminates the application process;
- the MDD application shall automatically restart and re-register with the MRP upon device reboot without requiring manual user intervention;
- the user information (Clause 5) shall clearly state that powering off the host device will interrupt MDS operation and may delay alarm transmission.

The responsible organisation's deployment risk assessment (Annex E) should document whether a software-only MDD provides adequate power-off protection for the intended deployment context.

4.1.10 Alarm Notification Requirements

4.1.10.1 MDD On-Device Notification

Upon trigger of any personal alarm, the MDD shall provide notification to the wearer in accordance with the device's configured Notification Mode.

Two Notification Modes are defined:

- **Standard Mode (default):** the MDD shall provide multi-modal notification including audible alert (minimum 85 dB(A) at 1 metre), visual alert (LED or screen indicator in red, flashing at minimum 0.5 Hz), haptic/vibration alert, and on-screen status display (where the device has a screen).
- **Covert Mode (refer Clause 4.2.3A):** the MDD shall provide haptic-only confirmation to the wearer. The audible alert and visible visual alert are suppressed. A discreet visual indicator visible only to the wearer (such as a low-luminance LED on the device's body-facing surface) is permitted.

The Notification Mode shall be configured at the time of deployment by authorised personnel in accordance with the deployment risk assessment (Annex E). Changing the Notification Mode shall require authorised personnel access.

4.1.10.2 MRP Notification

Upon receipt of an alarm transmission, the MRP shall immediately generate an audible alert of minimum 75 dB(A), display a prominent visual alarm notification, and where the MRP is a mobile application, generate a push notification using the highest-priority notification channel available.

4.1.10.3 Escalation and Notification Redundancy

The MDS shall support a configurable multi-tier escalation chain. A minimum of three escalation tiers shall be configurable.

4.1.10.4 Notification Delivery Confirmation

The MRP shall confirm delivery of alarm notifications to all configured recipients and log any delivery failures. Where SMS or voice call delivery cannot be confirmed, the system shall retry a minimum of three times.

4.1.10.5 Test Alarm Notifications

The MDS shall support the transmission and receipt of test alarm notifications that exercise the full notification chain without generating a real emergency response.

4.2 Requirements for Mobile Duress Devices (MDD)

4.2.1 Mandatory Automatic Alarm Capability

In addition to the mandatory voluntary alarm trigger (Emergency Activation Button), every MDD shall be equipped with at least one automatic alarm mechanism. The minimum required automatic alarm type shall be either Tilt/Position Alarm or Inactivity/No-Motion Alarm.

4.2.2 Pre-Alarm Capability

The MDD shall be capable of generating a pre-alarm before triggering any automatic personal alarm. The pre-alarm shall be resettable directly on the MDD without requiring network connectivity.

4.2.3 On-Site Audible Alert

Where the MDD is configured in Standard Mode (Clause 4.1.10.1), the audible alert specified in Clause 4.1.10.1 shall be emitted upon trigger of any personal alarm. The audible output shall be a minimum of 85 dB(A) at 1 metre.

Where the MDD is configured in Covert Mode (Clause 4.2.3A), the audible alert is suppressed. The MDD shall not produce any audible output upon alarm trigger that would be discernible to a person in the vicinity of the wearer.

4.2.3A Covert Duress Mode

Every MDD supplied for use in any of the deployment contexts listed in Clause 4.2.3A.1 shall support Covert Duress Mode as defined in Clause 4.1.10.1. Covert Duress Mode shall be available as a configurable option in all other deployments.

4.2.3A.1 Mandatory Covert Mode Deployments

Covert Duress Mode shall be the default Notification Mode in any MDS deployed in the following contexts:

- a personal safety deployment for a person identified as being at risk of family or domestic violence, or subject to a personal safety order, intervention order, or equivalent;
- a custodial officer or staff member duress deployment in any correctional facility;
- a personal duress deployment for a worker in any role where the responsible organisation's deployment risk assessment (Annex E) identifies covert operation as necessary to wearer safety, including but not limited to mental health crisis response, child protection field work, drug and alcohol services, and family violence services.

4.2.3A.2 Functional Requirements in Covert Mode

When operating in Covert Mode, the MDD shall:

- trigger and transmit all configured alarms in accordance with Section 4.1, identical in form and content to Standard Mode transmission;
- provide haptic confirmation to the wearer that the alarm has been triggered, of a duration and pattern distinguishable from haptic notifications used for other purposes (such as low battery or check-in reminders);
- provide haptic confirmation to the wearer when the MRP acknowledges the alarm (refer Clause 4.2.5);
- not emit any audible signal upon alarm trigger, alarm transmission, or alarm acknowledgment;
- not emit any externally visible visual signal upon alarm trigger, alarm transmission, or alarm acknowledgment, save for any low-luminance indicator on the device's body-facing surface that is not visible to a person facing the wearer.

4.2.3A.3 Activation Discreetness in Covert Mode

Where an MDD is supplied for a deployment in which Covert Duress Mode is the default (Clause 4.2.3A.1), the manufacturer shall provide at least one method for triggering a voluntary personal alarm that does not require the wearer to make a movement or gesture readily identifiable to an observer as activation of an alarm device. Acceptable methods include, but are not limited to: long-press of a concealed control; pre-defined motion gesture; pre-defined sequence of inputs; or activation through a paired discreet accessory.

The 15 mm minimum activation axis specified in Clause 4.2.10 (glove-operable controls) does not apply to a covert activation method. Where a separate non-covert Emergency Activation Button is also provided on the same device, that button shall comply with Clauses 4.2.9, 4.2.10, and 4.2.11.

4.2.4 Alarm Transmission and Voice Link

Upon triggering a personal alarm, the MDD shall transmit the alarm to the MRP, and where the MDD has voice capability (MDD-V), a voice communication link shall be automatically established.

4.2.5 Alarm Reset Requires MRP Acknowledgment

A triggered personal alarm on the MDD shall only be resettable after receipt of an acknowledgment from the MRP. Direct reset on the MDD alone without MRP authorisation is not permissible.

4.2.6 Battery Performance and Lifecycle Requirements

4.2.6.1 Minimum Operational Battery Life

Device Type	Minimum Battery Life	Includes
MDD (standard, no voice)	24 hours	Active GPS, network registration, all alarm sensors
MDD-V (with voice communication)	16 hours	As above plus 60 minutes of voice communication
MDD for remote/rural deployment	72 hours	Active positioning, network registration, alarm sensors
MDD with active alarm state (sustained)	4 hours minimum	Full alarm state: audible alert, repeated transmission, GPS active

Table 3 — Minimum Battery Life Requirements

4.2.6.2 Low Battery Warning

A low battery warning shall be issued when the remaining charge falls to 20% of rated capacity. The battery state percentage shall be reported to the MRP at least once every 60 minutes.

4.2.6.3 Battery Charge Time

The MDD shall reach at least 80% charge capacity within 2 hours and full charge within 4 hours.

4.2.6.4 Battery Cycle Life

The rechargeable battery shall maintain at least 80% of its rated capacity after a minimum of 500 full charge/discharge cycles.

4.2.6.5 Battery Degradation Monitoring

Where the MDD uses a smart battery management system (BMS), the estimated battery health should be reported to the MRP. When battery health falls below 70%, the MDD shall generate a technical alarm.

4.2.6.6 Battery Replacement

Where the battery is user- or technician-replaceable, the replacement procedure should be documented. Following battery replacement, the device shall automatically initiate a functional self-test.

4.2.6.7 Battery Safety

Battery cells and battery management systems shall comply with AS/NZS 62133.2:2021. Devices shall incorporate over-charge, over-discharge, over-temperature, and short-circuit protection.

4.2.7 Daily Automated Functional Test

The MDD shall automatically perform a functional test of all active alarm mechanisms and the geolocation function at intervals not exceeding 24 hours of continuous operation.

4.2.8 Pre-Deployment Testing and Commissioning

Before an MDD is placed into operational service, a pre-deployment functional test shall be performed and recorded. This requirement applies to every individual device and cannot be satisfied by batch or sample testing.

4.2.9 Emergency Button Identification and Design

The Emergency Activation Button on the MDD shall be red in colour. All operating controls shall be clearly labelled.

4.2.10 Glove-Operable Controls

All emergency alarm controls shall be operable while the wearer is wearing standard industrial or medical protective gloves. Button dimensions shall not be smaller than 15mm in the activation axis.

4.2.11 Accidental Activation Prevention

The Emergency Activation Button shall be protected against unintentional activation caused by contact with surfaces, clothing, or incidental pressure.

4.2.12 Secure Configuration

Operational settings and alarm thresholds of the MDD shall be modifiable only by authorised personnel, using a secure access method.

4.2.13 Secure Body Attachment

The MDD shall be designed for secure attachment to the wearer's person.

4.2.14 Fall Detection Performance (Where Claimed)

Where a manufacturer claims Fall Detection capability, the false positive rate shall not exceed 2 per 24-hour period and the false negative rate shall not exceed 10% across the defined test scenario set.

4.2.15 GPS/Location Fix Time

The time to first location fix from device wake-up shall not exceed 60 seconds under clear-sky conditions. The achieved accuracy shall meet the ≤ 5 metre threshold.

4.2.16 Device Labelling

The following information shall be clearly legible, permanently affixed, and durable on each MDD: manufacturer name, model designation, serial number/UDI, IP protection rating, RCM mark, battery type and voltage, manufacturing date, and where applicable TGA ARTG entry number.

4.2.17 Environmental and Mechanical Protection

4.2.17.1 IP Rating

MDDs shall have a minimum ingress protection rating of IP54. For outdoor, water-exposed, or clinical wet-area environments, a minimum of IP65 or IP67 is required.

4.2.17.2 Operating Temperature Range

The MDD shall operate within its full specification across an ambient temperature range of -10°C to +55°C.

4.2.17.3 Drop and Impact Resistance

MDDs shall withstand a free-fall drop of 1.5 metres onto a concrete surface, tested in accordance with AS/NZS IEC 60068.2.31:2019, with two impacts on each of three perpendicular axes.

4.3 Requirements for the Monitoring and Response Platform (MRP)

4.3.1 Alarm Differentiation

The MRP shall visually and audibly differentiate between personal alarms (voluntary and automatic) and technical alarms. Each alarm type shall be displayed distinctly and unambiguously.

4.3.2 Acoustic Alarm Reset

The acoustic alert in the MRP for any received alarm shall be manually resettable by an operator. The visual indicator for each device alarm shall only be resettable after the alarm has been acknowledged for that specific device.

4.3.3 Real-Time Location Display

The MRP shall display the geolocation of an alarming MDD on a map interface within the alarm notification. Historical location trails should be available for playback for a minimum of 7 days.

4.3.4 Voice Communication (MDD-V)

Where the MDS includes voice capability, the MRP shall establish a duplex voice connection with the alarming MDD-V automatically upon receipt of a personal alarm.

4.3.5 Alarm Logging and Audit Trail

The MRP shall log all personal and technical alarms with the following minimum data fields: date and time of alarm trigger, MDD identity, alarm type, geolocation, date and time of MRP receipt, date and time of operator acknowledgment, date and time of alarm reset, and operator ID. Alarm logs shall be retained for a minimum of 12 months. Export to CSV or PDF format should be supported.

4.3.6 MRP Power Supply and Availability

Where the MRP is hosted on dedicated hardware, it shall be supplied by two independent power sources. The backup power source shall maintain MRP operation for a minimum of 4 hours.

For cloud-hosted MRP deployments, the platform availability shall meet the following requirements:

Deployment Risk Level	Minimum Availability	Maximum Permissible Downtime (per calendar month)
Standard deployments	99.9%	43 minutes
High-risk deployments (DV, custodial, acute clinical)	99.95%	22 minutes

Table 5 — Cloud-hosted MRP availability requirements.

Availability shall be measured as follows:

- **Measurement window:** one calendar month (UTC), calculated as (total minutes in month minus downtime minutes) divided by total minutes in month.
- **Downtime definition:** any period exceeding 60 consecutive seconds during which the MRP is unable to receive, process, and display alarm transmissions from registered MDDs.
- **Excluded periods:** scheduled maintenance windows (maximum 4 hours per calendar month, notified to all Responsible Organisations at least 72 hours in advance); force majeure events affecting the underlying cloud infrastructure provider across an entire availability zone; and periods during which the Responsible Organisation's own network prevents connectivity to the MRP.
- **Attribution:** where the MRP provider relies on a third-party cloud infrastructure provider (e.g. AWS, Azure, GCP), the MRP provider remains accountable for the stated availability target. Infrastructure provider outages that are not excluded under the force majeure provision above count as MRP downtime.
- **Reporting:** the MRP provider should publish monthly availability reports to Responsible Organisations. Reports should include total downtime, root cause for any incident exceeding 5 minutes, and confirmation of compliance with the applicable availability target.

4.3.7 Data Security and Privacy

The MRP shall comply with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the Notifiable Data Breaches scheme. For deployments in New Zealand, the MRP shall comply with the Privacy Act 2020 (NZ). The following minimum security requirements apply:

- **Encryption in transit:** all data transmitted between MDD and MRP, and between MRP components, shall be encrypted using TLS 1.2 or later.
- **Encryption at rest:** all stored alarm data, location data, and user identity data shall be encrypted at rest using AES-128 or stronger.
- **Access control:** access to personal information held by the MRP shall be restricted to authorised personnel with a documented need to access.

Data residency and cross-border disclosure: The MRP provider shall take reasonable steps to ensure that personal information (including location data and alarm records) is stored and processed within Australia or New Zealand. Where personal information is disclosed to an overseas recipient (APP 8), the MRP provider shall:

- ensure the overseas recipient is subject to a law or binding scheme substantially similar to the APPs (APP 8.2(a)), or obtain the informed consent of the Responsible Organisation (APP 8.2(b));
- disclose in its product documentation and privacy policy the countries in which personal information may be stored or processed;
- maintain contractual arrangements with overseas recipients that require them to handle personal information in accordance with the APPs.

NOTE: This clause adopts the accountability model established by APP 8 (Australia) and Information Privacy Principle 12 (NZ), which impose obligations on the disclosing entity rather than mandating a geographic location restriction. In Australia, the MRP provider remains accountable under the Privacy Act 1988 for any act or practice of an overseas recipient that would breach the APPs, unless an exception under APP 8.2 applies. In New Zealand, the MRP provider must ensure that personal information disclosed to a foreign person or entity will be adequately protected under the Privacy Act 2020 (NZ), section 193, before disclosure occurs.

4.3.8 MRP Labelling and Identification

The following information shall be clearly visible: name and address of the software/platform provider, product/platform name and version number, and date of last update.

5 User Information

Every MDS shall be accompanied by documentation that enables safe and effective use of the product. Documentation shall be in English. Where the intended user population includes non-English speakers, documentation should be translated into the relevant language(s).

User documentation shall include at a minimum:

1. Name and business address of the manufacturer and/or Australian or New Zealand sponsor
2. Model designation and ARTG number (if applicable)
3. Clear listing of technical specifications, including battery life, alarm types supported, IP rating, operating temperature range, and network compatibility
4. Complete user manual including operating instructions, alarm activation and reset procedures, pre-alarm cancellation, and network status indicators
5. Instructions for charging and battery replacement (if applicable)
6. Maintenance and self-test requirements
7. Instructions for configuration by authorised personnel
8. Warning notices and safety precautions, including limitations of GPS accuracy, network coverage dependencies, and conditions under which automatic alarms may not trigger
9. Contact details for technical support and fault reporting
10. Explanation of all symbols, indicators, lights, and sounds used on the device

NOTE: For devices regulated as medical devices by the TGA, Instructions for Use (IFU) shall comply with the requirements of Schedule 3 of the Therapeutic Goods (Medical Devices) Regulations 2002.

6 Conformity Testing

This section specifies the testing requirements for verifying conformity of mobile duress systems with the requirements of this standard. Conformity testing is divided into system-level testing (Section 6.2), which evaluates the end-to-end performance of the complete MDS including the MDD, communication network, and MRP, and device-level testing (Section 6.3), which evaluates the individual MDD against the requirements of Section 4.2.

All testing shall be conducted by an accredited testing laboratory. For testing in Australia, laboratories shall hold NATA accreditation for the relevant test methods. For testing in New Zealand, laboratories shall hold IANZ accreditation. Test reports from ILAC-recognised bodies in other jurisdictions may be accepted at the discretion of the relevant regulatory authority.

Manufacturers and suppliers seeking to demonstrate conformity with this standard shall submit a complete MDS (including MDD, MRP software, and all communication infrastructure) for testing. Partial testing of individual components does not satisfy the conformity requirements of this standard.

6.1 General

The purpose of conformity testing is to verify that an MDS product meets all requirements specified in this standard. All requirements shall be verified by measurement-based test methods unless they can be satisfactorily confirmed by documented functional testing or verified by inspection of technical documentation.

Testing shall be conducted by an accredited testing laboratory. For testing in Australia, laboratories shall hold NATA accreditation. For testing in New Zealand, laboratories shall hold IANZ accreditation. Test reports from ILAC-recognised bodies in other jurisdictions may be accepted at the discretion of the relevant regulatory authority.

6.2 System-Level Testing (MDS)

6.2.1 Response Time Verification

Compliance with all response times specified in Table 1 shall be demonstrated by direct end-to-end time measurement across a minimum of 10 test activations per alarm type. The measurement shall be conducted using calibrated timing instrumentation with a resolution of at least 100 milliseconds. The worst-case measured value across all 10 activations shall not exceed the limits in Table 1.

6.2.2 Functional Testing

All functions specified in Clauses 4.1.2 through 4.1.10 shall be demonstrated through documented functional testing.

6.2.3 Electrical Safety

Electrical safety of the MDD shall be verified in accordance with AS/NZS 62368-1. Radio frequency compliance shall be verified in accordance with ACMA requirements.

6.2.4 User Documentation Review

User documentation shall be reviewed for completeness against the requirements of Clause 5.

6.3 Device-Level Testing (MDD)

6.3.1 Potentially Explosive Atmospheres (IECEx)

Where the MDD is intended for use in potentially explosive atmospheres, IECEx certificates from a body accredited under the IECEx Scheme shall be provided.

6.3.2 Device Labelling Verification

The markings on the MDD shall be checked for completeness against Clause 4.2.16. The durability of inscriptions shall be tested in accordance with AS/NZS 62368-1:2022, Section F.3.10.

6.3.3 IP Rating Testing

IP testing shall be conducted in accordance with AS/NZS 60529 in an unpowered state.

6.3.4 Temperature Range Testing

Temperature testing shall be performed in accordance with AS/NZS IEC 60068.2.14:2020 at ambient temperatures of (-10 ± 3)°C and (+55 ± 3)°C. The exposure duration at each extreme shall be 3 hours.

6.3.5 Drop Test

The drop test shall be conducted with a drop height of 1.5 metres onto a concrete surface, with two drops on each of three perpendicular axes (six drops total).

6.3.6 Fall Detection Algorithm Testing (Where Claimed)

Where fall detection is claimed, conformity with Clause 4.2.14 shall be verified by structured scenario-based testing conducted in accordance with the following normative protocol.

6.3.6.1 Reference Test Protocols

The test scenario set shall be derived from one or more of the following published fall detection evaluation protocols:

- Bagalà F, Becker C, Cappello A, et al. (2012). *Evaluation of accelerometer-based fall detection algorithms on real-world falls.* PLoS ONE 7(5):e37062. (FARSEEING project protocol)
- Sucerquia A, López JD, Vargas-Bonilla JF (2017). *SisFall: A Fall and Movement Dataset*. Sensors 17(1):198. (SisFall protocol — 15 fall types, 19 ADL types)
- Bourke AK, van de Ven P, Gamber M, et al. (2012). *Assessment of waist-worn tri-axial accelerometer based fall-detection algorithms using continuous unsupervised activities.* 34th IEEE EMBS Conference.

The testing laboratory shall declare which protocol(s) are used. Where a proprietary test set is used, it shall be documented to a level of detail that permits independent reproduction by another accredited laboratory.

6.3.6.2 Minimum Test Scenario Set

The test scenario set shall include, at minimum, the following 20 scenarios performed by each test subject:

Category	Scenarios	Count
Forward falls	Forward fall onto knees then floor; forward fall with arm protection; forward trip and fall	3
Backward falls	Backward fall from standing; backward fall from sitting (chair slip); backward fall with rotation	3
Lateral falls	Lateral fall left; lateral fall right; lateral fall from bed height	3
Syncope / collapse	Vertical collapse (loss of consciousness simulation); slow collapse to knees then floor	2
Activities of daily living (non-fall)	Sitting down quickly; lying down on bed; bending to pick up object; stumble with recovery; vigorous walking; climbing stairs; clapping/reaching overhead; jumping; coughing while seated	9

Table 6.1 — Minimum fall detection test scenario set.

6.3.6.3 Test Subject Requirements

Testing shall be conducted with a minimum of three (3) test subjects representing at least two different body mass categories (BMI < 25 and BMI ≥ 25) and at least two different height categories (< 170 cm and ≥ 170 cm). Both male and female subjects shall be included. The demographic characteristics of all test subjects (age, sex, height, weight, BMI) shall be recorded and reported.

NOTE: Single-subject testing (n=1) is not sufficient for conformity assessment. The requirement for multiple subjects addresses the known sensitivity of accelerometer-based fall detection algorithms to body morphology and gait characteristics.

6.3.6.4 Test Conditions

- Falls shall be performed onto a padded surface (gymnastics mat, minimum 200 mm thickness) to prevent injury to test subjects.

- The MDD shall be worn in its intended wearing position (wrist, belt, lanyard, etc.) as specified by the manufacturer.
- Each scenario shall be performed a minimum of three (3) times per test subject.
- A rest period of at least 30 seconds should separate each scenario to allow sensor baselines to reset.
- Testing should be conducted at room temperature (20–25°C).

6.3.6.5 Pass Criteria

The MDD passes fall detection conformity testing if:

- The false negative rate (missed falls) across all fall scenarios and all test subjects does not exceed 10%.
- The false positive rate (false alarms from ADL scenarios), extrapolated to a 24-hour period of typical activity, does not exceed 2 false alarms per 24 hours.

Results shall be reported per-scenario and per-subject, with aggregate pass/fail determination. The testing laboratory should report the detection latency (time from impact to alarm trigger) for each detected fall.

6.3.7 Location Accuracy Verification

- **Tier 1 (outdoor GPS):** GPS accuracy verified at minimum five test positions; mean error shall not exceed 5 metres.
- **Tier 2 (indoor room-level):** Correct room or zone identification verified at minimum ten positions; correct identification rate shall be at least 95%.
- **Tier 3 (indoor sub-metre):** Mean positioning error shall not exceed 1 metre; 95th percentile error shall not exceed 1.5 metres.
- **Tier 4 (remote/satellite):** GPS accuracy per Tier 1 requirements; age-of-fix timestamp mechanism verified.

7 Declaration of Conformity and Marking

7.1 Declaration of Conformity

Manufacturers or Australian sponsors shall issue a written Declaration of Conformity for each MDS product, confirming that the product meets all applicable requirements of this standard. The declaration shall include:

- Product name and model number
- Manufacturer name and address
- Australian or New Zealand sponsor name and address (if different from manufacturer)
- Reference to this standard: DR AS/NZS 5765.1:2026
- List of other standards or technical regulations with which the product complies
- Name and signature of the authorised signatory
- Date of declaration

Declarations of Conformity shall be made available to regulators and customers upon request and should be retained for a minimum of 5 years from date of last supply.

7.2 Certification Mark

Products that have been verified by an accredited third-party testing body as conforming to this standard may carry a certification mark administered by the certifying body. Products supplied in Australia shall carry the RCM (Regulatory Compliance Mark). Products supplied in New Zealand shall comply with the applicable New Zealand Electrical (Safety) Regulations 2010 and RSM requirements. The RCM mark is recognised in both Australia and New Zealand under the Trans-Tasman Mutual Recognition Arrangement (TTMRA).

8 Regulatory Pathway and Intended Submissions

8.1 Standards Australia / Standards New Zealand Pathway

Following close of public consultation and review by the independent technical panel (refer Foreword: Governance and Independence), this draft is intended to be submitted to Standards Australia under the New Standards Project (NSP) process, and concurrently to Standards New Zealand for joint development as an AS/NZS standard. The submission will be made jointly by RTLS Intelligence Pty Ltd and the confirmed co-sponsors, and will include:

- the revised draft incorporating consultation outcomes;
- a Net Benefit assessment addressing the matters specified in Standards Australia's NSP Policy (and equivalent Standards New Zealand requirements), including stakeholder need, evidence base, alternatives considered, and estimated costs and benefits of compliance;
- the full public record of consultation submissions and the responses of the drafting parties;
- a derivation annex tracing each quantitative requirement to its source authority;
- disclosure of commercial interests of all co-sponsors.

Standards Australia and Standards New Zealand will determine, in accordance with their own policies and processes, whether to approve a New Standards Project, and if approved, the appropriate technical committee, scope, and timeline. RTLS Intelligence Pty Ltd does not represent or warrant that this draft will be adopted in any form, in whole or in part.

8.2 Therapeutic Goods Administration (TGA)

Some products within scope of this standard may constitute medical devices under the Therapeutic Goods Act 1989 (Cth). Personal alarm devices marketed for aged care, post-acute care, or fall prevention may attract Class I or Class IIa classification depending on their intended purpose and claims. Manufacturers and sponsors are advised to consult the TGA's guidance on Software as a Medical Device (SaMD) where the MDS includes software-based clinical decision support, fall risk assessment, or health monitoring functions.

For products supplied in New Zealand, the equivalent regulatory body is Medsafe. The Therapeutic Products Act 2023 (NZ) is expected to modernise the regulatory framework for medical devices in New Zealand upon commencement.

8.3 Safe Work Australia, WorkSafe New Zealand, and WHS Regulators

RTLS Intelligence Pty Ltd intends to submit this standard to Safe Work Australia for consideration as a supporting technical reference for any Code of Practice, guidance material, or regulatory instrument relating to the use of mobile duress systems in Australian workplaces. State and Territory WHS regulators, each of which administers its own WHS legislation substantially based on the Model WHS Act, will also be engaged to ensure the standard supports consistent regulatory expectations across all Australian jurisdictions.

In New Zealand, RTLS Intelligence Pty Ltd intends to engage with WorkSafe New Zealand for consideration of this standard as a supporting reference under the Health and Safety at Work Act 2015 (NZ) and the Health and Safety at Work (General Risk and Workplace Management) Regulations 2016 (NZ). The HSWA 2015 imposes a primary duty of care on persons conducting a business or undertaking (PCBUs) to ensure, so far as is reasonably practicable, the health and safety of workers — including through the provision of adequate monitoring and emergency response systems where workers are exposed to isolation or personal safety risks.

8.4 Australian Communications and Media Authority (ACMA)

All MDDs covered by this standard are radiocommunications devices and must comply with ACMA technical standards, including the Radiocommunications (Radio Communications Equipment) Standard 2021 and applicable labelling and compliance marking requirements. For products supplied in New Zealand, the equivalent regulatory body is Radio Spectrum Management New Zealand (RSM), and devices must comply with the Radiocommunications Act 1989 (NZ) and associated regulations.

8.5 New Zealand Regulatory Pathway

As an AS/NZS joint standard, this standard will be submitted to Standards New Zealand concurrently with submission to Standards Australia. RTLS Intelligence Pty Ltd intends to engage with the following New Zealand bodies:

- Standards New Zealand, for joint development as an AS/NZS standard
- WorkSafe New Zealand, as the primary workplace health and safety regulator

- Ministry of Health New Zealand and Te Whatu Ora (Health New Zealand), for healthcare and aged care deployment contexts
- Radio Spectrum Management New Zealand (RSM), for radiocommunications compliance
- Office of the Privacy Commissioner New Zealand, for alignment with the Privacy Act 2020 (NZ)
- Medsafe, for medical device regulatory considerations
- Health Quality and Safety Commission New Zealand (HQSC), for quality and safety alignment
- Accident Compensation Corporation (ACC), for injury prevention alignment
- Whaikaha (Ministry of Disabled People), for disability services deployment contexts

New Zealand stakeholders are specifically encouraged to provide feedback during this consultation period on any requirements that may interact with New Zealand-specific legislation or operational conditions.

8.6 Commencement and Transition

Upon adoption of this standard:

- **New products:** comply in full from the date of adoption
- **Existing products in active deployment:** comply within 24 months of adoption
- **Products awaiting market release:** comply within 12 months of adoption

Non-conformances that represent an immediate risk to worker safety shall be remediated within 90 days of identification, regardless of the transition period.

Annex A (Informative): Known Market Deficiencies and Evidence Base

A.0 Methodology and Limitations

The market analysis summarised in this annex was conducted by RTLS Intelligence Pty Ltd between March 2024 and February 2026. The methodology, scope, and limitations are disclosed below to enable readers to assess the weight of the evidence independently.

A.0.1 Scope of Analysis

- **Products assessed:** 14 mobile duress and personal alarm products commercially available in Australia and New Zealand, sourced from 11 manufacturers across 5 countries of origin.
- **Selection method:** products were selected on the basis of market availability, advertised use in occupational safety or aged care contexts, and representation of the major technology categories (cellular, LPWAN, BLE/RTLS, satellite). Selection was not randomised.
- **Testing party:** all functional and performance testing was conducted by RTLS Intelligence Pty Ltd personnel. No independent laboratory was engaged for the market analysis phase. RTLS Intelligence Pty Ltd acknowledges that this introduces a potential perception of bias, and invites submissions identifying any specific finding that a submitter considers inaccurate.

A.0.2 Testing Conditions

- Alarm response time testing was conducted over live commercial networks (Telstra, Optus, Vodafone) in metropolitan Sydney and regional NSW locations.
- Fall detection testing used a structured scenario set of 20 fall types (5 forward, 5 backward, 5 lateral, 5 controlled lowering) performed by a single adult male tester (78 kg, 178 cm) on a padded surface.
- Battery life testing was conducted under continuous operational conditions: active GPS acquisition at 60-second intervals, network registration maintained, all alarm sensors active, no voice calls unless the device was voice-capable (in which case, 10 minutes of voice per 8-hour period).

- Geolocation accuracy was assessed by comparing reported coordinates against surveyed reference points using a Trimble R12i GNSS receiver.

A.0.3 Limitations

- The sample of 14 products is not exhaustive. Products not assessed may perform differently.
- Testing was conducted by the drafting party, not an independent laboratory. Results have not been independently verified.
- Network conditions, firmware versions, and product configurations at the time of testing may differ from current market offerings.
- No manufacturer was given advance notice of testing or an opportunity to configure the device prior to assessment. Devices were tested in their default shipping configuration.
- Individual product names and manufacturers are not disclosed in this annex to avoid commercial prejudice. Detailed test reports are available for inspection by the independent technical review panel (refer Foreword: Governance and Independence) and by Standards Australia and Standards New Zealand upon request.

A.0.4 Commitment to Independent Verification

Following close of public consultation, the findings summarised in this annex will be submitted to the independent technical review panel for assessment. Where the panel determines that any finding requires independent verification before it can support a normative requirement, RTLS Intelligence Pty Ltd will fund testing by a NATA-accredited laboratory with relevant scope, and the results will be published in the next draft revision.

A.1 Alarm Transmission Failures

Of the 14 products assessed, 4 products (29%) failed to transmit a voluntary alarm within 60 seconds on at least one test occasion under conditions of marginal network coverage (signal strength ≤ −95 dBm RSRP). In 2 of these cases, the device provided no indication to the wearer or the monitoring platform that the alarm transmission had failed, leaving the wearer in an unmonitored state without their knowledge. A further 3 products (21%) exhibited intermittent transmission failures that were not reproducible on every test occasion.

A.2 Excessive Response Times

Voluntary alarm transmission times (measured from button press to alarm display in the MRP) ranged from 2.1 seconds to 47.3 seconds across the 14 products assessed. The median was 8.4 seconds; the 90th percentile was 31.2 seconds. In time-critical scenarios such as assault, medical emergency, or fall, the difference between a 5-second and a 45-second alarm delivery represents a meaningful increase in risk. Clause 4.1.1 and Table 1 establish mandatory response times by Network Class, with a maximum of 5 seconds for Class A voluntary alarms — a requirement that was met by 6 of the 14 products assessed (43%).

A.3 Inadequate Fall Detection

Of the 14 products assessed, 9 claimed fall detection capability. These 9 products were tested using the structured fall scenario set (A.0.2). Results: 2 products detected 18 of 20 falls (90%); 3 products detected 10–14 of 20 falls (50–70%); 2 products detected fewer than 5 of 20 falls (< 25%); 2 products failed to detect any fall in any scenario. False positive rates ranged from 0 to 11 per 24-hour period of normal wear. This standard defines fall detection as a separate alarm category (Clause 3.7.6) and establishes minimum performance requirements (Clause 4.2.14) including a maximum false positive rate of 2 per 24-hour period and a maximum false negative rate of 10% across the defined test scenario set.

A.4 No Geolocation in Alarm Data

Of the 14 products assessed, 5 products (36%) transmitted alarm payloads that contained no location data whatsoever — only a device identifier and alarm type. A further 4 products (29%) included location data that reflected the last GPS fix from between 20 minutes and 6 hours prior to the alarm, with no indication of fix age in the MRP display. Only 5 products (36%) included a current or near-current location fix (< 5 minutes old) with an accuracy estimate. Clause 4.1.3 requires that the most recently acquired location be included in every alarm transmission, along with identification of the technology used, an estimate of accuracy, and the age of the fix.

A.5 Insufficient Battery Life

Battery life under operational test conditions (A.0.2) ranged from 4.2 hours to 38 hours across the 14 products assessed. Published manufacturer specifications for the same products ranged from 12 hours to 96 hours — representing overstatement factors of 1.5× to 4.8× relative to measured operational performance. The median overstatement factor was 2.3×. Section 4.2.6 establishes battery life requirements that must be demonstrated under defined operational test conditions, not standby or manufacturer-selected conditions.

A.6 Data Security and Privacy Gaps

Analysis of network traffic from 14 MDS platforms identified: 3 products (21%) transmitting location data over unencrypted HTTP connections; 5 products (36%) storing alarm and location records on infrastructure located outside Australia without disclosure in product documentation; 2 products (14%) with no encryption at rest for stored alarm records. Under the Privacy Act 1988 (Cth) and the Notifiable Data Breaches scheme, the organisations deploying these systems carry compliance obligations that the platform's practices placed at risk. Clause 4.3.7 mandates encryption in transit and at rest, Australian data residency as the default, and compliance with the Notifiable Data Breaches scheme.

Annex B (Informative): Relationship to Referenced German Standards

This Australian draft standard has been informed by and substantially aligned with DIN VDE V 0825-1 (VDE V 0825-1):2025-10 and DIN VDE V 0825-11 (VDE V 0825-11):2023-02. The table below reflects the multi-class and multi-tier structure introduced in this Australian standard, which extends the single-requirement approach of the German source documents.

Requirement	German Standard	This Australian Standard (DR AS/NZS 5765.1:2026)
Voluntary alarm response time	≤ 60 s (VDE V 0825-11, single requirement)	Tiered by Network Class (Clause 4.1.1, Table 1): Class A (Cellular/IP/RTLS): ≤ 5 s Class B (LPWAN): ≤ 45 s Class C (Satellite IoT): ≤ 90 s
Automatic alarm response time	≤ 120 s (tilt/ position)	Tiered by Network Class (Clause 4.1.1, Table 1): Class A: ≤ 90 s Class B: ≤ 120 s Class C: ≤ 180 s
Deployment suitability constraints	Not addressed (single technology assumed)	Class B/C restricted by deployment context (Clause 4.1.1B); Class C prohibited as sole MDS where response within 90 s is required; deployment risk assessment mandatory
Drop test height	1.0 m	1.5 m onto concrete (Clause 4.2.17.3, 6.3.5)
Minimum IP rating	IP52 / IP54	IP54 minimum (Clause 4.2.17.1); IP65/IP67 required for outdoor, water-exposed, or clinical wet-area environments
Fall Detection Alarm	Not defined as separate category	Defined as separate alarm type (Clause 3.7.6); performance criteria: ≤ 2 false positives/24 h, ≤ 10% false negatives (Clause 4.2.14); normative test protocol (Clause 6.3.6)
Data security / privacy	Not addressed	Encryption in transit (TLS 1.2+) and at rest (AES-128+); Privacy Act 1988 compliance; data residency accountability (Clause 4.3.7)
Cloud platform availability	Not addressed	99.9% standard / 99.95% high-risk; measured over calendar month with defined exclusions (Clause 4.3.6)
Alarm log retention	1 month	12 months (Clause 4.3.5)

Requirement	German Standard	This Australian Standard (DR AS/NZS 5765.1:2026)
Battery life	≥ 12 hours	Tiered by device type (Clause 4.2.6.1, Table 3): Standard MDD: 24 hours MDD-V (with voice): 16 hours Remote/rural MDD: 72 hours Active alarm state: 4 hours minimum
Location accuracy	Localisation required (single requirement)	Four-tier structure (Clause 4.1.3A, Table 4): Tier 1 (outdoor): ≤ 5 m (95th percentile) Tier 2 (indoor general): room-level (≤ 50 m² zone) Tier 3 (indoor high-accuracy): ≤ 1 m (95th percentile) — memory care, locked dementia units, acute mental health, high-dependency aged care Tier 4 (remote): GPS/GNSS with age-of-fix timestamp
Covert duress mode	Not addressed	Mandatory in DV, custodial, and high-risk worker contexts (Clause 4.2.3A); haptic-only confirmation; discreet activation methods exempt from 15 mm glove-operability requirement
Smartphone MDD support	Not in scope	Software-only MDDs in scope (Clause 3.2 NOTE); persistent foreground service required; technical alarm on force-close/power-off (Clause 4.1.9)
Notification modes	Audible alert only	Standard Mode (85 dB(A) + visual + haptic) and Covert Mode (haptic only); configurable by deployment context (Clause 4.1.10.1)

Table B.1 — Comparison with Referenced German Standards. All clause references are to this Australian standard (DR AS/NZS 5765.1:2026).

Annex C (Informative): Bibliography and Further Reference

The following documents, while not normative references to this standard, provide useful background, guidance, and context for implementers, manufacturers, and regulators.

C.1 German Technical Standards (Informative Source Documents)

- DIN VDE V 0825-1 (VDE V 0825-1):2025-10, *Surveillance systems — Wireless personal emergency signal systems for hazardous lone working — Part 1: Product and test requirements*
- DIN VDE V 0825-11 (VDE V 0825-11):2023-02, *Surveillance systems — Wireless personal emergency signal systems for lone workers — Part 11: Product and test requirements for personal emergency signal systems using public telecommunications networks*

C.2 Australian Government and Regulatory Guidance

- Safe Work Australia, *Workplace Health and Safety Statistics Australia: 2022-23*
- Safe Work Australia, *Work-related Traumatic Injury Fatalities Australia* (annual series)
- Safe Work Australia, *Model Code of Practice — How to Manage Work Health and Safety Risks* (2022)
- Safe Work Australia, *Guidance on the Work Health and Safety Laws* (2022)
- ACMA, *Radiocommunications (Radio Communications Equipment) Standard 2021*
- ACMA, *Buying and using radiocommunications devices — Compliance guide* (current edition)
- TGA, *Guidance: Regulation of Medical Devices, Overview* (2023)
- TGA, *Guidance: Software as a Medical Device (SaMD)* (2024 edition)
- OAIC, *Notifiable Data Breaches Scheme: quarterly statistics*
- Australian Digital Health Agency, *National Digital Health Strategy 2023–2028*

C.2A New Zealand Government and Regulatory Guidance

- WorkSafe New Zealand, *Good Practice Guidelines: Working Alone* (current edition)

- WorkSafe New Zealand, *Introduction to the Health and Safety at Work Act 2015* (HSWA Special Guide)
- WorkSafe New Zealand, *Worker Engagement, Participation and Representation: Good Practice Guidelines*
- Ministry of Business, Innovation and Employment (MBIE), *Health and Safety at Work Strategy 2018–2028*
- Office of the Privacy Commissioner New Zealand, *Privacy Act 2020: Information Privacy Principles*
- Office of the Privacy Commissioner New Zealand, *Guidance: Privacy Impact Assessments*
- Radio Spectrum Management New Zealand (RSM), *General User Radio Licence for Short Range Devices* (current)
- Te Whatu Ora (Health New Zealand), *Digital Health Strategic Plan*
- Te Whatu Ora, *Health and Disability Services Standards NZS 8134:2021*
- Medsafe, *New Zealand Medical Device Register (NZMDR)*
- Medsafe, *Guidance: Classification of Medical Devices under the Medicines Act 1981 (NZ)*
- Health Quality & Safety Commission New Zealand (HQSC), *Window on the Quality of Aotearoa New Zealand's Health Care*
- Accident Compensation Corporation (ACC), *Falls Prevention Strategy* (informative, relevant to fall detection MDS deployments)
- ACC, *New Zealand Injury Prevention Strategy*
- Whaikaha (Ministry of Disabled People), *New Zealand Disability Strategy 2016–2026*
- Office for Seniors, *Better Later Life — He Oranga Kaumātua 2019 to 2034* (NZ Positive Ageing Strategy)
- New Zealand Aged Care Association (NZACA), *Aged Residential Care Industry Profile* (current edition)

C.3 Industry and Occupational Health References

- DGUV Information 212-139, *Emergency call options for lone workers* (Germany)
- DGUV Rule 112-139, *Use of personal emergency signal systems* (Germany)
- Safe Work Australia, *Hazardous Manual Tasks Code of Practice* (2022)

- Aged Care Act 2024 (Cth)
- Aged Care Quality and Safety Commission, *Strengthened Aged Care Quality Standards* (effective 1 July 2024)
- NDIS Quality and Safeguarding Framework, *Practice Standards*
- ANMF, *Position Statement: Lone Worker Safety* (current), noting that ANMF guidance addresses the broader healthcare worker safety context including duress systems in clinical settings

C.4 Technical and Security References

- NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*
- ETSI EN 303 645, *Cyber Security for Consumer Internet of Things: Baseline Requirements*
- GSMA TS.34, *IoT Security Guidelines for Network Operators*
- 3GPP TS 22.261, *Service requirements for the 5G system*, *Stage 1* (informative reference, relevant to 5G-connected MDS devices)

Annex D (Informative): Drafting Transparency and Collaborative Development

This annex provides a transparency disclosure regarding the development of this standard, the organisations involved, the acknowledged limitations of the current draft, and the collaborative pathway forward. It is included to ensure stakeholders can assess the document's provenance and the governance arrangements that apply to its further development.

D.1 Drafting Origin and Acknowledgment

This Industry Consultation Draft was prepared by RTLS Intelligence Pty Ltd, an Australian company operating in the real-time location systems and personal safety technology sector. RTLS Intelligence Pty Ltd is a participant in the market that this standard is intended to regulate.

RTLS Intelligence Pty Ltd acknowledges that the preparation of a draft standard by a single market participant carries a perceived risk of conflict of interest, regardless of the technical merits of the document or the good faith of the drafters. This annex, together with the Governance and Independence section of the Foreword, addresses that risk explicitly and structurally.

D.2 Collaborative Development Pathway

This standard is not intended to remain the work of a single organisation. The following collaborative arrangements are in place or being established for the next revision and formal submission:

- **Co-sponsorship:** Prior to formal submission to Standards Australia and Standards New Zealand, this draft will be co-sponsored by one or more independent organisations, which may include an Australian university research group, a peak industry body in alarm monitoring, aged care, disability services, or worker safety, and/or a non-competing operator or end-user organisation. Co-sponsors will participate in the review of public submissions, the preparation of revised drafts, and the formal submission.
- **Independent Technical Review Panel:** All public submissions will be reviewed by an independent panel comprising representatives from a NATA/IANZ-accredited testing laboratory, a tertiary research institution, an end-user sector, and a relevant regulatory body or worker representative organisation. RTLS Intelligence Pty Ltd will participate as

the drafting party but will not chair the panel and will not have a determinative vote on contested clauses.

- **Standards Australia / Standards New Zealand governance:** The final standard, if adopted, will be developed under the established technical committee processes of Standards Australia and Standards New Zealand. RTLS Intelligence Pty Ltd does not represent or warrant that this draft will be adopted in any form.

D.3 Pre-Release Engagement

Prior to and during the public consultation period, RTLS Intelligence Pty Ltd is engaging or intends to engage with the following organisations and bodies across Australia and New Zealand. This engagement is intended to ensure the standard reflects the regulatory, operational, and safety requirements of both jurisdictions and all relevant sectors.

Standards Bodies

- **Standards Australia** — to discuss the New Standards Project (NSP) process, confirm the standard pathway, and identify the appropriate technical committee;
- **Standards New Zealand** — concurrent engagement for joint development as an AS/NZS standard through the New Zealand Standards Executive;
- **Prospective co-sponsors** — at least one co-sponsor from each country is intended to be named in the next draft revision.

Australian Regulatory and Government Bodies

- **Safe Work Australia** — on the applicability of the standard to workplace lone worker deployments and alignment with model WHS Codes of Practice;
- **State and Territory WHS regulators** (WorkSafe Victoria, SafeWork NSW, Workplace Health and Safety Queensland, WorkSafe WA, SafeWork SA, WorkSafe Tasmania, NT WorkSafe, WorkSafe ACT) — on jurisdiction-specific implementation and deemed-to-satisfy pathways;
- **Therapeutic Goods Administration (TGA)** — on the regulatory classification of MDS products with medical device characteristics (fall detection, health monitoring);
- **Australian Communications and Media Authority (ACMA)** — specifically on the treatment of duty-cycle-constrained bearers (Network Class C) under the class licence regime;

- **Office of the Australian Information Commissioner (OAIC)** — on the privacy implications of location tracking and alarm data collection under the Privacy Act 1988;
- **Aged Care Quality and Safety Commission** — on the applicability to residential aged care personal alarm systems and alignment with the Strengthened Aged Care Quality Standards;
- **National Disability Insurance Agency (NDIA)** — on the applicability to NDIS-funded assistive technology and personal safety supports;
- **Australian Digital Health Agency** — on interoperability with national digital health infrastructure where MDS devices include health monitoring functions.

New Zealand Regulatory and Government Bodies

- **WorkSafe New Zealand** — on the applicability of the standard to New Zealand workplace health and safety obligations under the Health and Safety at Work Act 2015;
- **Ministry of Business, Innovation and Employment (MBIE)** — as the parent body of the New Zealand Standards Executive, on alignment with the NZ standards development framework;
- **Radio Spectrum Management New Zealand (RSM)** — on radiocommunications compliance under the Radiocommunications Act 1989 (NZ);
- **Office of the Privacy Commissioner New Zealand** — on alignment with the Privacy Act 2020 (NZ) and Information Privacy Principles;
- **Medsafe** — on medical device regulatory considerations under the Therapeutic Products Act 2023 (NZ);
- **Health Quality & Safety Commission New Zealand (HQSC)** — on patient safety and quality improvement implications for aged care and disability services;
- **Te Whatu Ora (Health New Zealand)** — on healthcare deployment contexts and alignment with the Health and Disability Services Standards NZS 8134:2021;
- **Accident Compensation Corporation (ACC)** — on the potential for MDS to reduce injury severity and rehabilitation costs in workplace and community settings;
- **Office for Seniors / Ministry of Social Development** — on the applicability of personal alarm systems to the ageing population strategy and community-based care;
- **Whaikaha (Ministry of Disabled People)** — on disability services deployment contexts and alignment with the NZ Disability Strategy 2016–2026;
- **New Zealand Aged Care Association (NZACA)** — on practical deployment considerations for residential aged care facilities in New Zealand.

Industry and Sector Bodies (Australia and New Zealand)

- **Australian Security Industry Association Limited (ASIAL)** — on alarm monitoring industry practices and integration with existing monitoring centre infrastructure;
- **New Zealand Security Association (NZSA)** — on the New Zealand security and monitoring industry perspective;
- **Australian Nursing and Midwifery Federation (ANMF)** — on lone worker safety for healthcare workers and clinical deployment contexts;
- **New Zealand Nurses Organisation (NZNO)** — on healthcare worker safety in New Zealand clinical environments;
- **A peak body in the family and domestic violence sector** (e.g. WESNET, DVConnect, Our Watch in Australia; Women's Refuge, Shine in New Zealand) — on the Covert Duress Mode framing, to ensure the language and deployment-context list reflect sector practice;
- **Aged & Community Care Providers Association (ACCPA)** — on Australian aged care provider perspectives and practical deployment considerations;
- **Australian Council of Trade Unions (ACTU)** — on worker representative perspectives regarding lone worker safety technology;
- **New Zealand Council of Trade Unions (NZCTU)** — on New Zealand worker representative perspectives;
- **Communications Alliance (Australia)** — on telecommunications industry alignment and network technology considerations;
- **IoT Alliance Australia** — on IoT device standards alignment and interoperability;
- **Relevant university research groups** — with expertise in occupational health and safety, assistive technology, wireless communications, or gerontology (both Australian and New Zealand institutions).

D.4 Acknowledged Outstanding Work

The following items have been identified as requiring further development in subsequent revisions. They are disclosed here so that stakeholders may provide targeted feedback and so that the limitations of the current draft are transparent:

Item	Description	Priority
Derivation Annex	A traceability annex linking each quantitative threshold (response times, battery life, accuracy) to its source authority, published evidence, or engineering justification	High
Cost-Benefit Analysis	A formal cost-benefit assessment as required by Standards Australia's NSP Net Benefit policy (and equivalent Standards New Zealand requirements), including estimated compliance costs for manufacturers and deploying organisations	High
Fall Detection Test Protocol	A detailed fall detection test scenario set with reference to published clinical protocols (e.g. Bourke et al., Bagalà et al.)	Medium
Privacy Act Update	Citation update to reflect the Privacy Act 1988 amendments effective 2024, particularly regarding location data as sensitive information	Medium
TGA Pathway Clarification	Clarification of the Therapeutic Goods Administration regulatory pathway for the medical-device subset of MDS products (particularly fall detection and health-monitoring features)	Medium
Smartphone MDD Reconciliation	Further refinement of the interaction between Clause 3.2 (scope including smartphone MDDs) and hardware-specific requirements throughout Section 4	Medium

Stakeholders are encouraged to provide submissions on any of the above items. Feedback identifying additional gaps or proposing specific drafting solutions is particularly valued.

D.5 Invitation to Participate

This standard will be stronger for the breadth and diversity of organisations that contribute to its development. RTLS Intelligence Pty Ltd invites expressions of interest from any organisation willing to participate in the collaborative development process, whether as a co-sponsor, a member of the independent review panel, a contributor of technical expertise, or a provider of real-world deployment data.

Expressions of interest may be submitted through the consultation portal alongside regular submissions, or directed to the contact details provided in the Industry Consultation Notice at the front of this standard.

Annex E (Informative): Deployment Risk Assessment Framework

This annex defines the deployment risk assessment referenced throughout this standard (Clauses 4.1.1B, 4.1.9, 4.1.10.1, and 4.2.3A). The deployment risk assessment is a documented evaluation conducted by the Responsible Organisation (Clause 3.15) prior to deploying an MDS, and reviewed at intervals not exceeding 12 months or following any material change in deployment conditions.

E.1 Purpose

The deployment risk assessment ensures that the MDS configuration selected — including Network Class, Notification Mode, location accuracy tier, and device form factor — is appropriate to the specific risks faced by MDS Wearers in the deployment context. It provides a traceable record of the decisions made and the rationale for those decisions.

E.2 Minimum Contents

The deployment risk assessment shall document, at minimum, the following:

Item	Description	Relevant Clause(s)
1. Deployment context	Description of the environment, population of MDS Wearers, nature of risks (violence, falls, isolation, medical emergency), and operational conditions (indoor/outdoor, remote/urban, shift patterns).	1, 3.14
2. Network Class selection	The Network Class (A, B, or C) selected for the deployment, with rationale. Where Class B or C is selected, documentation that the extended response times are acceptable for the identified risk profile. Where Class C is selected, confirmation that the deployment does not involve immediate physical threats requiring response within 90 seconds.	4.1.1A, 4.1.1B
3. Notification Mode selection	Whether Standard Mode or Covert Mode is configured, with rationale. For deployments in the mandatory covert contexts (Clause 4.2.3A.1), confirmation that Covert Mode is the default.	4.1.10.1, 4.2.3A
4. Location accuracy tier	The Location Accuracy Tier (1–4) applicable to the deployment environment, and confirmation that the selected MDD meets the accuracy requirement for that tier.	4.1.3A, Table 4
5. Software-only MDD assessment	Where a software-only MDD (smartphone application) is deployed, documentation that the power-off protection mechanisms are adequate for the deployment context, and that wearers are informed of the limitations.	4.1.9, 3.2 NOTE
6. Response capability	Confirmation that the monitoring and response arrangements (MRP staffing, escalation chain, emergency service integration) are adequate to respond within the timeframes achievable by the selected Network Class.	4.3, 4.1.10.3
7. Wearer consultation	Evidence that MDS Wearers (or their representatives) have been consulted on the deployment configuration, consistent with WHS consultation obligations under the Work Health and Safety Act 2011 (Cth) or the Health and Safety at Work Act 2015 (NZ), as applicable to the jurisdiction of deployment.	General

Item	Description	Relevant Clause(s)
8. Review schedule	The date of next scheduled review, which shall be no later than 12 months from the date of the assessment or the date of any material change in deployment conditions, whichever is earlier.	General

Table E.1 — Minimum contents of the deployment risk assessment.

E.3 Responsibility and Governance

The deployment risk assessment shall be prepared or commissioned by the Responsible Organisation. It shall be signed by a person with authority to make deployment decisions on behalf of that organisation. Where the MDS is deployed by a third party (e.g. a managed service provider deploying on behalf of an employer), the Responsible Organisation retains accountability for the adequacy of the risk assessment.

The deployment risk assessment should be made available to:

- MDS Wearers or their representatives upon request;
- WHS regulators upon request;
- the MDS supplier, where the supplier requires confirmation of appropriate deployment for warranty or support purposes.

E.4 Relationship to WHS Risk Assessment

The deployment risk assessment defined in this annex is not a substitute for the general risk assessment obligations under the Work Health and Safety Act 2011 (Cth), equivalent state/territory legislation, or the Health and Safety at Work Act 2015 (NZ). It is a supplementary, MDS-specific assessment that addresses the technical configuration decisions unique to mobile duress systems. Where the Responsible Organisation already conducts WHS risk assessments (or health and safety risk assessments under HSWA 2015) that address the matters in Table E.1, those assessments may satisfy this requirement provided they are documented and include the MDS-specific items.

E.5 Template Availability

A template deployment risk assessment document will be made available as a companion resource to this standard following close of the consultation period. The template is not normative and organisations may use any format that addresses the minimum contents specified in Table E.1.