Informationssicherheit Richtlinie für Dritte

Ersatz für: -

		Name	Abteilung	Datum
melecs	Erstellt/ geändert	Thomas P.	QMS	2024-06-07
	geprüft	Hermann L.	PI	2024-06-07
	freigegeben	Erich L.	SVP OP	2024-06-18

Inhaltsübersicht

1 Zweck des vorliegenden Dokumentes

Diese Richtlinie legt die organisatorischen Vorgaben und Regeln zur Informationssicherheit fest, die von Dritten beim Umgang mit Informationen der Melecs EWS GmbH Standorte in Österreich, im Folgenden: MELECS, zu beachten sind. Die Begriffe Informationen und Daten in diesem Dokument beziehen sich ausschließlich auf Informationen und Daten der MELECS. Dritte sind definiert als Vertragspartner, die aufgrund vertraglicher Beziehungen Produkte/Dienstleistungen mit Auswirkungen auf die Info. Sec. für MELECS liefern/erbringen. Diese Richtlinie gilt nicht für Kunden der MELECS.

Diese Richtlinie richtet sich an die Geschäftsleitung der Dritten. Die Geschäftsführung des Dritten hat sicherzustellen, dass ihre Mitarbeiter und Erfüllungsgehilfen, die Informationen der MELECS verarbeiten, auf diese Informationssicherheitsrichtlinie verpflichtet werden.

Dieses Dokument wendet sich mit den Sicherheitsanforderungen an drei Zielgruppen. Die folgende Tabelle zeigt, welche Zielgruppe durch welches Kapitel angesprochen wird.

Kapitel	Zielgruppe
4	Alle Info. Sec. Dritte
5	Dritte, die in der MELECS IT Infrastruktur arbeiten
6	Dritte, die MELECS Informationen außerhalb der Melecs IT Infrastruktur im Zugriff haben oder bereitstellen

Ein Dritter kann je nach Zusammenarbeitsmodell gleichzeitig zu mehreren Zielgruppen gehören.

2 Geltungsbereich

Diese Richtlinie ist gültig für die österreichischen MELECS-Standorte.

3 Allgemeine Sicherheitsbestimmungen an alle Dritte

3.1 Klassifikation von Informationen

Ziel der Klassifizierung ist es, die Informationen entsprechend ihrem Schutzbedarf in Stufen einzuteilen. Je nach Klassifizierung sind unterschiedliche Schutzmaßnahmen erforderlich.

Alle MELECS-Informationen müssen entsprechend ihrer Vertraulichkeit klassifiziert werden. Die Vertraulichkeitseinstufungen können sich zu bestimmten Meilensteinen ändern.

Werden Dokumente oder Informationen von Dritten für MELECS erstellt, ist die Einstufung nach Vertraulichkeit beim Ansprechpartner von MELECS zu erfragen und entsprechend zu kennzeichnen.

3.2 Weitere Vorgaben

- Informationssicherheitsvorfälle (z.B. auftretende Störungen, Verstöße gegen die Richtlinie, Cyber-Angriffe), die Informationen oder IT-Systeme des Auftraggebers betreffen, sind unter informationsecurity@melecs.com oder dem Melecs-Ansprechpartner unverzüglich, mit den für die Beurteilung der Kritikalität erforderlichen Informationen zu melden. Weitere Informationen zum Ereignis sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- Wird ein Angriff mithilfe von Schadsoftware vermutet oder entdeckt, dürfen die betroffenen IT-Geräte und Speichermedien nicht mehr zur Verarbeitung von MELECS-Informationen verwendet werden.
- Vermutete Verwundbarkeiten und Schwachstellen der IT-Systeme der MELECS sind unverzüglich an informationsecurity@melecs.com zu melden.
- Bei Verdacht auf Verlust von internen, vertraulichen oder geheimen Informationen des Auftraggebers ist dies unverzüglich dem Ansprechpartner von MELECS zu melden.
- Die Weitergabe von Daten oder Informationen an sonstige Dritte ist nur mit schriftlicher Genehmigung des Informationseigentümers zulässig.
- Dokumente und Speichermedien, die schutzwürdige Informationen der MELECS enthalten, sind vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff zu schützen. Sobald die Daten auf dem Speichermedium nicht mehr benötigt werden, sind sie dort sicher zu löschen. Nicht mehr benötigte Speichermedien sind physikalisch zu vernichten.
- Nicht durch MELECS gemanagte IT-Geräte müssen den Stand der Technik entsprechend abgesichert sein. Die fehlerfreie Verarbeitung der Informationen und der Schutz vor unbefugter Veränderung sind sicherzustellen.
- Bei allen Gesprächen und Datenübertragungen (einschließlich Telefongesprächen, Video- und Webkonferenzen), die vertrauliche oder streng vertrauliche Informationen von MELECS betreffen oder enthalten, ist sicherzustellen, dass diese nicht unbefugt abgehört oder mitgelesen werden können.
- Für Übersetzungen von Dokumenten, die vertrauliche oder streng vertrauliche Informationen der MELECS enthalten, dürfen insbesondere keine öffentlichen (im Sinne der Vertraulichkeit „unsicheren“) Internet-Übersetzungsdienste (u. a. mit AI-Methoden) verwendet werden. Eine Freigabe durch den Auftraggeber im Vorfeld ist erforderlich.

4 Zusätzliche Anforderungen an Dritte

Nachfolgend eine Auflistung von zusätzlichen Anforderungen an Dritte, die in der MELECS-Infrastruktur arbeiten.

4.1 Definition

Ein Dritter darf in der Melecs-Infrastruktur nur arbeiten, wenn:

- IT-Geräte (physische oder virtuelle Endgeräte) von MELECS zur Verfügung gestellt werden, oder
- die Anbindung über Remote-Access-Lösungen mit Zugriff auf das interne MELECS-Netzwerk erfolgt oder
- die Anbindung des Dritten direkt an das interne MELECS-Netzwerk erfolgt oder
- über das Internet bereitgestellte zugangsgeschützte Anwendungen von MELECS genutzt werden.

Dies gilt unabhängig davon, ob sich der Dritte an einem Standort von MELECS befindet.

4.2 Anforderungen

- Bei der Mitnahme von nicht durch MELECS-betreuten IT-Geräten auf das Betriebsgelände oder in Sicherheitsbereichen ist zu beachten, dass diese IT-Geräte nicht in das MELECS-Netzwerk (Ausnahme stellt das Gäste WLAN dar) eingebracht werden dürfen. Ausnahmen sind, wie unter Kapitel Nutzung von MELECS-Netzwerkdiensten4.5 beschrieben, geregelt.
- Von der MELECS-IT zur Verfügung gestellte IT-Geräte sind sachgerecht zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.
- Von der MELECS zur Verfügung gestellte IT-Geräte dürfen nur mit Genehmigung der MELECS vom Standort der MELECS entfernt werden.
- Die Bereitstellung oder Installation von Hard- und Software darf nur durch MELECS-IT durchgeführt oder veranlasst werden.
- Es darf nur die von MELECS zur Verfügung gestellte Hardware, Software und Speichermedien genutzt werden.
- Das Öffnen des von MELECS zur Verfügung gestellten IT-Gerätes und das Vornehmen von Änderungen an der Hardware (z.B. Ein-/Ausbau von Komponenten) und das Ändern von Sicherheitseinstellungen (z.B. im Webbrowser) ist ausschließlich der MELECS-IT gestattet. Das Entfernen von Nutzungsbeschränkungen (z.B. „Jailbreaking“ oder „Betriebssystem-Rooting“) ist nicht gestattet.
- Der Einsatz oder die nachträgliche Veränderung von Programmen ist nur mit Genehmigung der MELECS-IT zulässig.
- Auf den von MELECS zur Verfügung gestellten IT-Geräten dürfen ausschließliche MELECS-Daten verarbeitet werden.
- Jeder Dritte ist dafür verantwortlich, dass Informationen, Programme und IT-Geräte nur im Rahmen der jeweiligen Aufgabenstellung ordnungsgemäß eingesetzt und genutzt werden.
- Der Versand von nicht dienstlichen Informationen ist nicht gestattet.

- Die Nutzung privater Software und Daten auf den von MELECS zur Verfügung gestellten IT-Geräten ist nicht gestattet.
- Nicht mehr benötigte Hardware (z. B. Laptop, USB-Sticks, USB-Festplatten) und Software ist unverzüglich, spätestens jedoch bei Vertragsende zurückzugeben.
- Reparaturen von durch MELECS zur Verfügung gestellten IT-Geräten dürfen nur durch MELECS veranlasst werden.
- Der Verlust von durch MELECS zur Verfügung gestellter Hardware ist durch den jeweiligen Nutzer unverzüglich dem zuständigen Ansprechpartner und unter informationsecurity@melecs.com zu melden.
- IT-Geräte und -Datenträger, auf denen personenbezogene, vertrauliche oder streng vertrauliche Daten gespeichert sind, dürfen MELECS-Standorte nur verschlüsselt verlassen.

4.3 Umgang mit klassifizierten Informationen

Informationen dürfen nur einem berechtigten Personenkreis im Rahmen der vereinbarten Tätigkeiten und unter Einhaltung der entsprechenden Regelungen zugänglich gemacht werden. Dabei ist das Need-to-know-Prinzip zu beachten.

Zum Schutz interner, vertraulicher oder streng vertraulicher Informationen sind die entsprechenden IT-Geräte so einzurichten, dass der Zugriff durch Unbefugte verhindert und das Risiko der Einsichtnahme durch Unbefugte minimiert wird.

Informationen sind während ihres gesamten Lebenszyklus entsprechend ihrer aktuellen Vertraulichkeitseinstufung vor dem Zugriff Unbefugter zu schützen. Es gelten folgende Regeln:

Vertraulichkeitsstufe	Anforderung
Offen/Open	• Kennzeichnung: Keine Kennzeichnungspflicht – kann als OFFEN / OPEN gekennzeichnet werden • Vervielfältigung und Verteilung: keine Einschränkung • Speicherung: keine Einschränkung • Entsorgung: keine Einschränkung
Intern/ Internal	• Kennzeichnung: Keine Kennzeichnungspflicht – kann als INTERN / INTERNAL gekennzeichnet werden • Vervielfältigung und Verteilung: Nur an berechtigte Dritte im Rahmen der Tätigkeit bzw. Anwendungsbereichs • Speicherung: Schutz vor unautorisiertem Zugriff • Entsorgung: Gemäß ISO/IEC 21964, Schutzklasse 2 (Papier: Partikelgröße max. 160mm², Hardware: mehrfach zerteilt und verformt Partikelgröße max. 2000mm²)
Vertraulich/ Confidential	• Kennzeichnung: Angabe der Vertraulichkeitsstufe VERTRAULICH oder CONFIDENTIAL auf der ersten Seite des Dokuments • Vervielfältigung und Verteilung: Nur an eine beschränkte Gruppe von berechtigten Dritten im Rahmen der Tätigkeit sowie des Anwendungsbereichs UND nach vorheriger Genehmigung durch den Informationseigentümer, durch Melecs. Die Person, die die Information verteilt, ist für angemessene Verteilwege verantwortlich, um die Informationen und Daten vor unbefugtem Zugriff und/oder Mithören zu schützen. • Speicherung: Schutz vor unautorisiertem Zugriff. Zugriff nur für eine beschränkte Gruppe. Verschlüsselte externe Speichermedien.

	• Entsorgung: Gemäß ISO/IEC 21964, Schutzklasse 2 (Papier: Partikelgröße max. 160mm², Hardware: mehrfach zerteilt und verformt Partikelgröße max. 2000mm²) • Transport/Versand: Vertrauliche Dokumente müssen in verschlossenen, neutralen Umschlägen versendet werden. E-Mails nur mittels TLS Verschlüsselung.
Streng Vertraulich/ STRICTLY CONFIDENTIAL	• Kennzeichnung: Angabe der Vertraulichkeitsstufe STRENG VERTRAULICH oder STRICTLY CONFIDENTIAL auf jeder Seite des Dokuments • Vervielfältigung und Verteilung: Nur an eine sehr restriktiv begrenzte Gruppe (z.B. Namensliste) von berechtigten Dritten im Rahmen der Tätigkeit sowie des Anwendungsbereichs UND nach vorheriger Genehmigung durch den Informationseigentümer, durch Melecs. Alle Daten sind zu verschlüsseln. Je nach Anwendungsfall sind weitere technische bzw. organisatorische Sicherheitsmaßnahmen zu verwenden (z.B. Verbot von Weiterleiten und Ausdrucken). • Speicherung: Schutz vor unautorisiertem Zugriff. Zugriff nur für eine sehr restriktiv begrenzte Gruppe (z.B. geschlossene Nutzergruppe). Alle Daten sind verschlüsselt gespeichert. • Entsorgung: Gemäß ISO/IEC 21964, Schutzklasse 2 (Papier: Partikelgröße max. 160mm², Hardware: mehrfach zerteilt und verformt Partikelgröße max. 2000mm²) • Transport/Versand: Streng vertrauliche Dokumente müssen in verschlossenen, neutralen Außenumschlägen versendet werden. In diesen ist ein zweiter innerer Umschlag zu platzieren, welcher mit der Klassifikation „STRENG VERTRAULICH“ gekennzeichnet und geschützt ist. E-Mails nur mittels TLS Verschlüsselung. Dateien nur verschlüsselt über Melecs Cloud oder verschlüsselten PDF und Passwortweitergabe via SMS.

Die Vorgaben zum Umgang mit Informationen gelten ebenfalls für IT-Systeme.

4.4 Umgang mit Benutzeraccounts

Benutzer-Accounts und -Passwörter stellen den wesentlichsten Schutz gegenüber unberechtigtem Netzwerkzugang und unberechtigter Nutzung von Applikationen sowie Informationen dar.

Folgende Vorgaben beim Umgang mit Benutzer-Accounts und Passwörtern sind durch alle Benutzer zu befolgen:

- Nicht mehr benötigte Benutzer-Accounts oder Zugriffsberechtigungen sind umgehend dem zuständigen Ansprechpartner zu melden, damit diese gelöscht bzw. gesperrt werden können.
- Die Weitergabe von Authentifizierungsmitteln (z. B. Authenticator Apps) ist nicht gestattet.

Es ist von großer Bedeutung, dass sichere Passwörter verwendet werden und das Passwortgeheimnis gewahrt bleibt. Folgende Punkte sind zu beachten:

- Mindestlänge: 12 Zeichen
- Für Benutzerkonten mit erhöhten Rechten sollte die Mindestlänge auf 15 Zeichen erhöht werden.
- Komplexes Passwort besteht aus mindestens 3 der folgenden 4 Kriterien:
  - Großbuchstaben (A-Z)
  - Kleinbuchstaben (a-z)
  - Ziffern (0-9)
  - Sonderzeichen (#,!,& etc.)
- Änderung alle 360 Tage

- Die letzten 10 Passwörter dürfen nicht verwendet werden
- Die Änderung eines Passworts durch den Benutzer ist erst am nächsten Tag möglich
- Nach 10 Fehlversuchen bei der Passworteingabe wird der Domain Account für 30 Minuten gesperrt
- Das Passwort darf nicht den Kontonamen oder Teile des Namens des Benutzers enthalten

Wichtige Hinweise:

- Das Initial-Passwort ist unverzüglich abzuändern.
- Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor- und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für triviale Passwörter mit Zahlenkombinationen (z.B. Melecs123456!).
- Passwörter sollten nicht trivialen Tastaturkombinationen entsprechen, wie z.B. "Qwertzui12§" bei deutschen Tastaturen.
- Jeder Benutzer hat ausschließlich seine personalisierten Zugangsdaten zu verwenden. Die Verwendung von Gruppen-Accounts ist grundsätzlich nicht vorgesehen, Ausnahmen sind durch interne Prozesse freizugeben.
- Unter keinen Umständen dürfen Benutzer individuelle Passwörter an andere Benutzer, Vorgesetzte oder Außenstehende weitergeben.
- Bei der Eingabe von Passwörtern müssen Sie darauf achten, dass die Eingabe von anderen Personen nicht beobachtet werden kann.
- Passwörter dürfen unter keinen Umständen auf nicht vertrauenswürdigen Systemen oder bei einer unerwarteten Befehlszeile eingegeben werden.
- Passwörter dürfen nicht unverschlüsselt im Klartext gespeichert, aufbewahrt oder übertragen werden.
- Die Speicherung von dienstlichen Passwörtern/Zugangsdaten in sonstigen Passwortspeichern (z. B. von Browsern zur Auto-Vervollständigung) ist unzulässig.
- Trennen Sie private und geschäftliche Nutzung immer sauber und verwenden Sie stets unterschiedliche Passwörter für unterschiedliche Benutzerkonten
- Passwörter von Service-Accounts (d. h. Accounts für Machine-to–Machine-Kommunikation (M2M)) müssen eine Mindestlänge von 32 Zeichen aufweisen, komplex (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen) sein, mit einem sicheren Zufallsgenerator erzeugt und so konfiguriert sein, dass eine aktive Anmeldung durch den Benutzer mit diesen nicht möglich ist

4.5 Nutzung von MELECS-Netzwerkdiensten

Nur IT-Geräte der MELECS dürfen an das Netzwerk angeschlossen werden. (Ausnahme Gäste WLAN)

Die Verbindung von netzwerkfähigen, nicht von der MELECS-gemangten IT-Geräten mit dem MELECS-Netzwerk ist nur zulässig, wenn dieses Vorgehen für das jeweilige IT-Gerät explizit durch den Auftraggeber freigegeben wurde. Davor ist vom Dritten sicherzustellen, dass das einzubringende IT-Gerät, dem Stand der Technik entsprechend, abgesichert ist. Ausnahmen müssen von der MELECS–IT-Sicherheit im Vorfeld geprüft und durch den CIO oder seinem Vertreter freigegeben werden.

4.6 Zusätzliche Anforderungen bei mobiler Arbeit

Die Beschäftigten des Dritten haben in eigener Verantwortung dafür Sorge zu tragen, dass die einschlägigen Regelungen zur Informationssicherheit und zum Datenschutz bei mobiler Arbeit uneingeschränkt eingehalten werden. Arbeitsunterlagen, Daten und Informationen dürfen weder an öffentlichen Orten noch in Privaträumen für Unbefugte sichtbar und zugänglich sein und auch nicht mitgehört werden können.

Der Anschluss von Hardware (z. B. Maus, Tastatur, USB-Sticks) an die von MELECS zur Verfügung gestellte Hardware ist nur zulässig, wenn diese von MELECS zur Verfügung gestellt wurde.

Bildausgabegeräte (z.B. Monitore, Projektoren), die nicht von MELECS zur Verfügung gestellt werden, dürfen verwendet werden, wenn der Anschluss kabelgebunden erfolgt und keine Funkübertragung verwendet wird.

Von MELECS zur Verfügung gestellte IT-Geräte sind physisch gegen Diebstahl und Missbrauch zu schützen:

- Wird ein IT-Gerät unbeaufsichtigt in einem Fahrzeug zurückgelassen, muss dies so geschehen, dass es von außen nicht sichtbar ist.
- Bei Flug- und Bahnreisen sind IT-Geräte im Handgepäck zu transportieren.
- Ist ein IT-Gerät längere Zeit unbeaufsichtigt, muss es ausgeschaltet werden.

5 Zusätzliche Anforderungen an Dritte

Zusätzliche Anforderungen an Dritte, die Informationen der MELECS außerhalb der MELECS-IT-Infrastruktur im Zugriff haben oder bereitstellen.

Ein Dritter hat dann Informationen der MELECS außerhalb der MELECS-IT-Infrastruktur im Zugriff, wenn dieser MELECS-Informationen in seiner eigenen IT-Infrastruktur verarbeitet oder für die MELECS oder weitere Dritte im Auftrag der MELECS hostet.

5.1 Anforderungen

Es gelten die Regularien zur Informationssicherheit des Dritten, soweit nichts anderes vertraglich vereinbart wurde. Die bei der Lieferantenauswahl erhobenen Informationen zur Informationssicherheit sowie getroffenen Vereinbarungen können durch den Auftraggeber geprüft werden.

6 Sanktionen

Verstöße gegen diese Richtlinie werden im Einzelfall nach den geltenden gesetzlichen und vertraglichen Bestimmungen geprüft und entsprechend geahndet.

Abweichungen von dieser Richtlinie, die das Sicherheitsniveau beeinträchtigen, sind nur nach Rücksprache mit dem Ansprechpartner und Freigabe durch den CIO oder dessen Vertreter zulässig und stets zeitlich zu befristen.