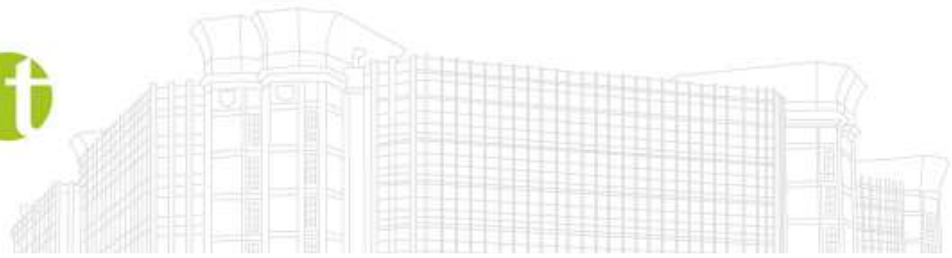


Security Checkliste

Security Checklist für die Benutzung des Führerscheinregisters über Portal Austria Zielgruppe: Fahrschulen, Automobilclubs, Prüfer, Aufsichtsorgane

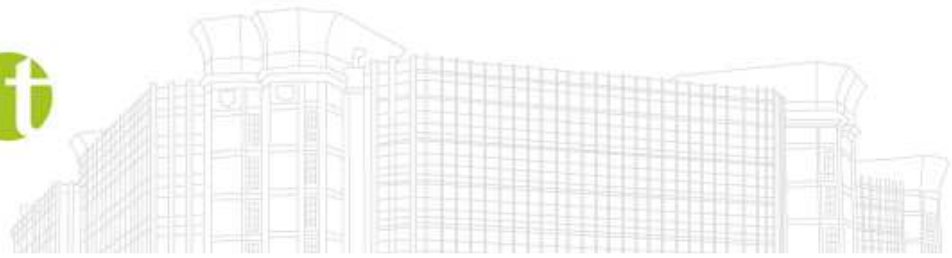
Version: 2.3
Erstellt am: 12.03.2018

Dokumentenparameter

Allgemeine Informationen	
Dokumententitel	Security Checkliste
Vertraulichkeitshinweis	FSR-intern
Beschreibung	Security Checklist für die Benutzung des Führerscheinregisters über Portal Austria Zielgruppe: Fahrschulen
Dokumentenverantwortlich	*Mag. Wolfgang Schubert bmvit*
Dokumentenart	
Review	
Review-Intervall	jährlich
Datum letzter Review	<Datum>
Gültigkeit	
Organisation	**bmvit**
Zielgruppe(n)	■ alle Mitarbeiterinnen und Mitarbeiter ☐ Führungskräfte ☐ Prozessverantwortliche
	■ freigegeben ☐ Entwurf / Überarbeitung ☐ archiviert
Freigabe durch	*bmvit*
Datum der Inkraftsetzung	12.03.2018

Version	**Datum**	**Autor/in**	**Änderung**
2.0	*22.01.2018*	*Josef Schmid*	*Änderungen gem. ges. Vorgaben*
2.1	*09.02.2018*	*Josef Schmid*	*Änderungen gem. Review bmvit, FSR WT*
2.2	*09.03.2018*	*Josef Schmid*	*Freigegebene Version*
2.3	*12.03.2018*	*Josef Schmid*	*Finales bmvit Review*

Inhaltsverzeichnis



Vorwort

Die vorliegende Checkliste stellt die in der Security Policy für die Benutzung des Führerscheinregisters über das Portal Austria beschriebenen Maßnahmen in übersichtlicher Form dar. Es wird aufgezeigt welche Maßnahmen unbedingt umgesetzt werden müssen, welche umgesetzt werden sollten und für welche eine Umsetzung empfohlen wird.
Die beschriebenen Sicherheitsmaßnahmen basieren auf geltenden bundesweiten Empfehlungen, insbesondere dem Österreichischen Informationssicherheitshandbuch in der Version 4.0.1 (https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf).

Die Checkliste ist als Ergänzung zur Security Policy zu sehen und kann z.B. als Basis für eine mögliche interne Überprüfung des Umsetzungsstatus herangezogen werden.

Maßnahmenkategorien:

Muss: Maßnahmen dieser Kategorie sind zur Gewährleistung der sicheren Nutzung des Führerscheinregisters über das Portal Austria unbedingt umzusetzen. Sie dienen zum Aufbau und zur Gewährleistung eines notwendigen "Grundschutz-Sicherheitsniveaus".
Soll: Maßnahmen dieser Kategorie sind erweiterte Grundschutzmaßnahmen. Eine Umsetzung wird dringend empfohlen.
Empfehlung: Maßnahmen dieser Kategorie sind eine gute und sinnvolle Ergänzung zu den beiden anderen Kategorien. Durch die Umsetzung dieser Maßnahmen in Kombination mit den Maßnahmen der Kategorien "Muss" und "Soll" kann ein gutes Sicherheitsniveau erreicht werden.

Maßnahmen

Die in der u.a. Tabelle angeführten Kapitel beziehen sich auf das bmvit Dokument

Security Policy Führscheinregister in der Version 2.4.

Kapitel 3	**Kennwortsicherheit und Authentifizierung**	**Maßnahmenkategorie**
Einhaltung der allgemeinen Nutzungsbedingungen des Portal Austria		Muss
Authentifizierung am Portal Autria nur durch starke Authentifizierung (Bürgerkarte bzw. Handysignatur!)		Muss
Kapitel 4	**Informationssicherheit am Arbeitsplatz**	**Maßnahmenkategorie**
Ist dafür gesorgt, dass Informationen vertraulich behandelt werden und unter keinen Umständen an unberechtigte Personen weitergegeben werden?		Muss
Sind alle Monitore so aufgestellt, dass keine unbefugte Einsichtnahme möglich ist bzw. falls dies nicht möglich ist, wird darauf geachtet, dass bei Arbeiten im Führerscheinregister keine unberechtigten Personen die Bildschirminhalte einsehen können?		Muss
Sind alle Benutzerinnen und Benutzer des Führerscheinregisters über die sichere Nutzung des Internets informiert?		Muss
Wird der Cache des Browsers beim Schließen gelöscht?		Muss
Werden regelmäßig Sicherheitsupdates durchgeführt? Ist sichergestellt, dass nur die dafür zuständigen Administratoren die erforderlichen Berechtigungen für die Installation und für Änderungen der Systemkonfiguration haben?		Muss
Sind alle Webbrowser sicher konfiguriert?		Muss
Wird das ”least privilege” Prinzip eingehalten? Ist sichergestellt, dass jede Mitarbeiterin bzw. jeder Mitarbeiter nur jene Berechtigungen besitzt, die zur Erfüllung der Aufgaben benötigt werden?		Muss
Werden Arbeitsstationen beim Verlassen gesperrt (z.B. kennwortgeschützter Bildschirmschoner)?		Muss
Sichere Verschlüsselung bei WLAN-Nutzung		Muss
Werden Ausdrucke aus dem Führerscheinregister versperrt aufbewahrt?		Muss

Werden alle verwendeten Software Programme vor ihrer Installation durch das Unternehmen freigegeben?		Empfehlung
Einsatz von Spam-Filtern für E-Mails		Empfehlung
Kapitel 5	**Virenschutz**	**Maßnahmenkategorie**
Werden alle Arbeitsstationen durch einen Virenschutz geschützt? Werden dessen Antivirus Signaturen regelmäßig aktualisiert?		Muss
Werden notwendige Schritte bei Verdacht auf Virenbefall eingeleitet? (Kontakt Systembetreuer, Administrator, etc.)		Muss
Werden sämtliche Kommunikationskanäle durch den Virenschutz überwacht?		Soll
Wird der Zugriff auf die Antivirensoftware durch ein Passwort geschützt?		Soll
Werden alle nicht benötigten Makrofunktionen deaktiviert?		Soll
Werden alle Arbeitsstationen, von welchen auf das Führerscheinregister zugegriffen wird regelmäßig vollständig auf Viren überprüft?		Soll
Kapitel 6	**(Personal) Firewall**	**Maßnahmenkategorie**
Werden alle Arbeitsstationen durch eine Firewall geschützt? (Personal Firewall oder Hardware Firewall)		Muss
Ist die Firewall entsprechend der Security Policy konfiguriert (Nur die Ports erlaubter Applikationen sind freigeschaltet, alle anderen Ports sind gesperrt)?		Soll
Einsatz eines mehrstufigen Schutzes bei der Verwendung von Hardware-Firewalls (zusätzliche Personal Firewalls auf den Arbeitsplatzrechnern)		Empfehlung
Einsatz von Hardware-Firewalls bei mehreren Arbeitsplatzrechnern in einem Netzwerk		Empfehlung
Kapitel 7	**Wartung und Entsorgung von Hard- und Software**	**Maßnahmenkategorie**
Werden Arbeitsplatzrechner regelmäßig gewartet (Updates, Patches, etc.)?		Muss
Werden alle Regelungen zur Fernwartung eingehalten (z.B. Nachvollziehbarkeit, Verschlüsselung, Überwachung, Dokumentation, etc:)		Muss / Soll (je nach Einzelregelung)
Werden alle Regelungen für Wartungsarbeiten im Haus eingehalten?		Muss / Soll (je nach Einzelregelung

Gibt es vertragliche Regelungen für die Fernwartung im notwendigen Umfang?		Muss
Werden alle Regelungen für externe Wartungsarbeiten eingehalten?		Muss / Soll (je nach Einzelregelung)
Ist gewährleistet, dass mit der Entsorgung von Datenträgern keine Daten nach außen gegeben werden? (Löschung, Vernichtung)		Muss
Kapitel 8	**Physikalische Sicherheit**	**Maßnahmenkategorie**
Ist der Zugang bzw. Zugriff auf Arbeitsstationen nur für befugte Personen möglich?		Soll
Ist sichergestellt, dass vertrauliche Informationen nicht frei liegengelassen werden um die Gefahr der Bekanntgabe an Dritte zu minimieren?		Muss
Gibt es Regelungen für den Verlust bzw. Diebstahl von Schlüssel?		Soll
Werden Fehldrucke aus dem Führerscheinregister bzw. nicht mehr benötigte Informationen in Papierform sicher vernichtet (Aktenvernichter, etc.)?		Muss
Kapitel 9	**Social Engineering**	**Maßnahmenkategorie**
Sind alle Mitarbeiterinnen und Mitarbeiter mit den Techniken und Angriffsszenarien von Sozial Engineering vertraut bzw. kennen diese die grundlegenden Sicherheitshinweise? Werden etwaige Angriffe diskutiert bzw. fließen die Ergebnisse in aktuelle Schulungen ein?		Soll
Kapitel 10	**Sicherheitssensibilisierung und Schulungen**	**Maßnahmenkategorie**
Verfügt jede Mitarbeiterin bzw. jeder Mitarbeiter über ein adäquates Sicherheitsbewusstsein und ein dementsprechendes Verhalten? Wird dies durch laufende (zumindest jährliche) Schulungen zur Informationssicherheit sichergestellt?		Soll
Kapitel 11	**Regelungen für Sicherheitsvorfälle**	**Maßnahmenkategorie**
Werden kritisch erscheinende Sicherheitsvorfälle an die zuständige Behörde gemeldet bzw. gibt es hierzu Regelungen?		Muss
Sind die Mitarbeiterinnen und Mitarbeiter auf Sicherheitsvorfälle sensibilisiert bzw. kennen Sie die Vorgehensweise bei einem diesbezüglichen Verdacht		Soll
Werden geeignete Maßnahmen auf Basis bereits eingetretener		Soll

Sicherheitsvorfälle getroffen (kontinuierliche Verbesserung?)		
Kapitel 12	**Nutzung der Applikation Führerscheinregister**	**Maßnahmenkategorie**
Werden nicht mehr benötigte Accounts an die entsprechenden Stellen gemeldet (z.B. nach Beendigung eine Dienstverhältnisses)?		Muss
Kennen die Mitarbeiterinnen und Mitarbeiter die Regelungen für die korrekte Nutzung der Applikation Führerscheinregister?		Muss
Wird beim Zugriff auf das Führerscheinregister regelmäßig das Zertifikat im Web-Browser auf Echtheit überprüft?		Soll