Baden-Württemberg

STAATLICHE LEHR- UND VERSUCHSANSTALT FÜR WEIN- UND OBSTBAU WEINSBERG

Leitlinie zur Informationssicherheit

Dokumentenverantwortlicher	Dienststellen-Leitung
Verfasser	Andy Höss, CISO
Kategorie	Leitlinie
Gültig ab	01.06.2021
Version	1.0
Status	verabschiedet
Klassifizierung	Öffentlich

Inhalt

1 Aufgabe, Ziel und Strategie der Informationssicherheit

Die Staatliche Lehr- und Versuchsanstalt für Wein- und Obstbau in Weinsberg (nachfolgend LVWO) betreibt praxisnahe Versuchsarbeit und bereitet Nachwuchs sowie Führungskräfte durch Aus- und Fortbildung auf ihre zukünftigen Aufgaben vor. Hinzu kommen Forschungsaufgaben und Labortätigkeiten. Die LVWO untersteht der Dienst- und Fachaufsicht des Ministeriums für Ländlichen Raum und Verbraucherschutz Baden-Württemberg (MLR). Digitalisierung und Informationstechnik haben für die Wahrnehmung dieser Aufgaben eine steigende Bedeutung und zunehmende Kritikalität. Die Sicherheit der Systeme ist für die Landesverwaltung von höchster Bedeutung und resultiert aus der Verpflichtung des Staates gegenüber den Bürgern und der Wirtschaft, verantwortungsvoll bei der Erhebung, Speicherung, Übermittlung und Nutzung von Daten und Informationen vorzugehen (Vgl. VwV Informationssicherheit, Absatz 1). Unachtsamkeit, Unsachgemäßer Einsatz oder rechtswidriger Umgang mit sensiblen Informationen oder Informationssystemen führt zu hohen Risiken und damit negativen Auswirkungen auf Reputation und Wirtschaftlichkeit der LVWO.

Aus diesem Grund werden sukzessiv die Schutzbedarfe von Informationen und Informationssystemen erhoben, sowie anschließend alle technischen und organisatorischen Maßnahmen zum Schutz von Vertraulichkeit, Verfügbarkeit und Integrität derselben ergriffen. Zielsetzung ist es dabei, ein angemessenes Niveau der Informationssicherheit zu erreichen sowie Risiken zu minimieren. Das Verhalten der Mitarbeiterinnen und Mitarbeiter spielt dabei eine besondere Rolle.

2 Management der Informationssicherheit

Die LVWO betreibt ein Informationssicherheits-Management-System (nachfolgend ISMS) nach ISO 27001 und BSI-IT-Grundschutz. Dessen Wirksamkeit wird durch technische und organisatorische Maßnahmen kontinuierlich gesteigert und durch regelmäßige Audits überprüft und verbessert.

Grundlage hierfür bilden nachfolgende Gesetze und Verordnungen:

- VwV „Informationssicherheit“ (Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit)

- „EGovG BW“ (Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden Württemberg)

- Informationssicherheitsleitlinie für den Geschäftsbereich des Ministeriums für Ländlichen Raum und Verbraucherschutz (MLR)

sowie die flankierenden Verwaltungsvorschriften „BITBW“, „IT-Organisation“ und „IT-Standards“ des Innenministeriums, geltende Rechtsvorschriften des Landes Baden-Württemberg sowie die Vorgaben der „CISO-Bestellungsurkunde“.

3 Elemente und Vorgaben der Informationssicherheit

Die Wahrung der Informationssicherheit durch verantwortungsbewussten Umgang mit anvertrauten Informationen und Informationssystemen ist Pflicht und Aufgabe aller Mitarbeiterinnen und Mitarbeiter der LVWO. Unabhängig von Stellung oder Aufgabenbereich sind Sie zur Wahrung und Weiterentwicklung der Informations-sicherheit verpflichtet. Externe und Dritte sind ebenso darauf hinzuweisen bzw. vertraglich zu verpflichten. Nachfolgende abstrakte Vorgaben gelten verbindlich und werden in Folgedokumenten konkretisiert.

- **Bewerten** Sie vor Beschaffung und Einsatz von Hard- und Software bzw. Cloudprodukten frühzeitig wirtschaftliche, rechtliche, ökologische und sicherheitsrelevante Aspekte des gesamten Produktlebenszyklus.

- **Verwenden** Sie für dienstliche Zwecke ausschließlich dienstliche Hardware und schützen Sie diese ausreichend gegen Missbrauch, Diebstahl, Beschädigung und Verlust.

- **Verwenden** Sie für dienstliche Zwecke ausschließlich dienstliche Software. Achten Sie dabei auf Software-Hygiene und konfigurieren Sie die Sicherheits-

einstellungen stets restriktiv. Achten Sie stets auf Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Informationen.

- **Bewerten** Sie zu verarbeitende Informationen (bspw. Persönliche Daten, Forschungsdaten, Vertragsdaten, Zugangsdaten, etc.) nach dem dafür notwendigen und gesetzlichen Schutzbedarf und ergreifen Sie angemessene Schutzmaßnahmen um Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten.

- **Achten** Sie auf Informations- und Daten-Hygiene indem Sie bspw. die Ansammlung und Verarbeitung privater/fremder Informationen in dienstlichen Informationssystemen vermeiden, dies regelmäßig überprüfen und handeln (löschen, archivieren, etc.) handeln.

- **Bewegen** Sie sich verantwortungsvoll im Internet und achten Sie darauf, dass ihre dienstlichen Kontaktdaten auf ein Minimum reduziert sind sowie diese restriktiv und möglichst verschleiert aufzufinden sind.

- **Beachten** Sie beim Umgang mit Informationen die Vorgaben DSGVO, BDSG, UrhG, die spezifischen Verwaltungsvorschriften und Gesetze der Landesverwaltung Baden Württemberg sowie vertragliche Verpflichtungen.

- **Nehmen** Sie Fehlermeldungen des Systems wie bspw. Windows-Warnmeldungen, Warnmeldungen der VirenScanner oder SPAM-Kennzeichnungen der BITBW unbedingt ernst und verständigen Sie bei allen Unregelmäßigkeiten umgehend IuK oder CISO.

4 Verantwortlichkeiten

Die Gesamtverantwortung der Informationssicherheit obliegt der Leitung der Dienststelle und kann nicht delegiert werden. Zur Unterstützung dieser Ziele ist ein Informationssicherheitsbeauftragter bzw. Chief Information Security Officer (CISO)

bestellt. Der CISO berichtet direkt dem Leiter der Dienststelle sowie dem CISO des Ressorts MLR (Ressort-CISO). Er ist dafür mit den notwendigen Ressourcen und Kompetenzen zur Aufgabenerfüllung ausgestattet und in dieser Rolle unabhängig und weisungsfrei.

5 Verstöße gegen die Informationssicherheit

Vorsätzliche oder grob fahrlässige Handlungen sowie Unterlassungen, welche die Vertraulichkeit, Verfügbarkeit und Integrität von Informationssystemen, Geschäftsprozessen und Informationen der LVWO beeinträchtigen sowie Verstöße gegen geltendes Recht werden nach geltenden rechtlichen Bestimmungen geahndet.

6 Geltungsbereich

Diese Leitlinie gilt für alle Mitarbeiterinnen und Mitarbeiter sowie auch externe Dritte wie bspw. Dienstleister, Studierende oder Gäste der Organisation. Sie umfasst ferner alle organisationseigenen IT-Systeme, Geschäftsprozesse, Informationen und Dokumente.

7 Inkraftsetzung und Bekanntgabe

Die Leitlinie zur Informationssicherheit tritt mit Wirkung zum 01.06.2021 in Kraft und ist allen Beschäftigten und Dritten in geeigneter Weise bekannt zu geben.

Weinsberg, den 20.05.2021

Dr. Dieter Blankenhorn — Andy Höss

Amtsleiter — Dienststellen-CISO