					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P29					Dokumenttitel: **Richtlinie für Testdaten und Testumgebungen**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Relevant für die sichere Planung und Steuerung von Testdaten und Testumgebungen
ISO/IEC 27002:2022	Maßnahmen 8.28–8.29	Deckt den sicheren Umgang mit Testdaten und den Schutz von Testumgebungen ab
NIST SP 800-53 Rev. 5	SA-11, SC-28, SC-32	Behandelt Entwicklertests und -bewertungen, den Schutz ruhender Daten und die Integrität
EU-DSGVO	Artikel 5, 25, 32	Deckt Datenminimierung, Datenschutz durch Technikgestaltung und Sicherheit der Verarbeitung in Testkontexten ab
EU NIS2	Artikel 21(2)(e), (h)	Bezieht sich auf sichere Entwicklungs- und Testpraktiken
EU DORA	Artikel 9	Betrifft IKT-Systeme und -Protokolle sowie die Sicherheit von Testdaten
COBIT 2019	DSS05, BAI07	Behandelt die Verwaltung von Sicherheitsdiensten sowie Änderungsannahme und -überführung

1. Zweck

1.1. Diese Richtlinie legt verbindliche Anforderungen für die Verwaltung von Testumgebungen und Testdaten fest, um Sicherheit, Vertraulichkeit und betriebliche Integrität über den gesamten Lebenszyklus der Softwareentwicklung und des Testens sicherzustellen.

1.2. Sie dient dazu, unbefugten Zugriff, Datenabfluss und die Kontaminierung von Produktivsystemen durch unzureichend verwaltete Testumgebungen oder durch die Nutzung von Echtdaten zu Testzwecken zu verhindern.

1.3. Die Richtlinie schreibt den sicheren Umgang mit zu Testzwecken verwendeten Daten, die Härtung der Testinfrastruktur sowie rollenbasierte Zugriffskontrollen vor und ist an geltenden regulatorischen und vertraglichen Verpflichtungen ausgerichtet.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für sämtliche Testumgebungen, Daten, Werkzeuge und Prozesse, die organisationsweit für Software-, System-, Anwendungs- und Infrastrukturtests verwendet werden.

2.2. Sie umfasst:

2.2.1. lokal bereitgestellte Testumgebungen, Testumgebungen in der Cloud oder über Plattformen Dritter bereitgestellte Testumgebungen

2.2.2. Testdaten, die für Funktions-, Leistungs-, Regressions- und Sicherheitstests verwendet werden

2.2.3. manuelle, skriptgestützte oder automatisierte Tests, z. B. in CI/CD-Pipelines

2.2.4. sämtliches Personal, das an Testaktivitäten beteiligt ist, einschließlich interner Teams, Lieferanten und Auftragnehmern

2.3. Die Richtlinie gilt unabhängig von der Kritikalität des Systems, dem Anwendungstyp oder davon, ob die Entwicklung intern oder ausgelagert erfolgt.

3. Ziele

3.1. Die Verwendung von Produktivdaten, sensitiven Daten oder regulierten Daten, z. B. personenbezogenen Daten oder Karteninhaberdaten, in Testumgebungen zu verhindern, sofern diese nicht anonymisiert wurden oder keine ausdrückliche Genehmigung vorliegt.

3.2. Eine vollständige Netzwerksegmentierung und -isolation sowie Zugriffstrennung zwischen Test- und Produktivumgebungen sicherzustellen, um unbefugten Datenzugriff oder die Kontaminierung von Systemen zu vermeiden.

3.3. Verschlüsselung, Maskierung oder die Erzeugung synthetischer Daten verbindlich vorzuschreiben, wenn für Testzwecke repräsentative Daten erforderlich sind.

3.4. Die Wahrscheinlichkeit von Verstößen gegen Anforderungen, der Offenlegung von Kundendaten oder betrieblichen Störungen infolge unsicherer Testdaten oder Testumgebungen zu reduzieren.

3.5. Den Umgang mit Testdaten an Industriestandards wie ISO, NIST und COBIT sowie an Vorschriften wie DSGVO, NIS2 und DORA auszurichten.

4. Rollen und Verantwortlichkeiten

4.1. Chief Information Security Officer (CISO)

4.1.1. Ist Eigentümer dieser Richtlinie und setzt technische und administrative Schutzmaßnahmen für Testdaten und Testumgebungen durch.

4.1.2. Genehmigt die Verwendung von Echtdaten oder sensitiven Daten zu Testzwecken bei Vorliegen einer angemessenen Begründung und kompensierender Kontrollen.

4.2. QA-/Test-Leitung

4.2.1. Koordiniert die Testplanung und stellt sicher, dass sämtliche Testaktivitäten die Anforderungen dieser Richtlinie einhalten.

4.2.2. Validiert für jede Testphase die ordnungsgemäße Trennung, den Zugriff und die Datenaufbereitung.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1. Diese Richtlinie muss jährlich überprüft und bei Bedarf aktualisiert werden, um Folgendes zu berücksichtigen:

9.1.1. Änderungen regulatorischer Anforderungen, z. B. DSGVO, DORA oder NIS2

9.1.2. Einführung neuer Testwerkzeuge, Plattformen oder Automatisierungspipelines

9.1.3. interne Auditfeststellungen oder Empfehlungen aus Vorfällen

9.1.4. Erweiterungen von Entwicklungs- oder QA-Prozessen, die den Umgang mit Testdaten oder die Nutzung von Testumgebungen verändern

9.2. Der CISO ist dafür verantwortlich, die Überprüfung in Zusammenarbeit mit folgenden Stellen einzuleiten:

9.2.1. QA-/Test-Leitung

9.2.2. DevOps- und Infrastrukturmanagement

9.2.3. Anwendungsentwicklungsteams

9.2.4. Datenschutzbeauftragter (DPO) und Rechtsabteilung

9.3. Alle Überarbeitungen müssen:

9.3.1. versionskontrolliert und im zentralen Dokumentenrepository gespeichert werden

9.3.2. betroffenen Personen über formale Kanäle mitgeteilt werden, z. B. über ISMS-Benachrichtigungen oder Team-Unterweisungen

9.3.3. mit Aktualisierungen zugehöriger technischer Standards, Kontrollen und Betriebsverfahren verknüpft sein

9.4. Anlassbezogene außerplanmäßige Überprüfungen müssen unverzüglich nach Folgendem durchgeführt werden:

9.4.1. Datenabfluss oder Datenschutzverletzung im Zusammenhang mit Testumgebungen

9.4.2. Audit-Nichtkonformität im Zusammenhang mit dem Umgang mit Testdaten

9.4.3. wesentlichen Änderungen rechtlicher Verpflichtungen oder der IT-Architektur

10. Verwandte Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist eng mit den folgenden Richtlinien verzahnt, um einen sicheren und regelkonformen Umgang mit Testdaten und Testumgebungen sicherzustellen:

10.1.1. P1 – Informationssicherheitsrichtlinie: Legt übergeordnete Sicherheitsgrundsätze fest, die den Schutz von Testdaten und die Verwaltung von Testumgebungen steuern.

10.1.2. P5 – Änderungsmanagement-Richtlinie: Gilt für die Erstellung, Aktualisierung und Außerbetriebnahme von Testumgebungen sowie von Bereitstellungspipelines.

10.1.3. P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Steuert die Auswahl von Testdaten und die Durchsetzung sensitivitätsbasierter Kontrollen.

10.1.4. P14 – Richtlinie zur Datenaufbewahrung und Entsorgung: Definiert Aufbewahrungsfristen und Anforderungen an die sichere Entsorgung von Testdatenbeständen.

10.1.5. P15 – Richtlinie für Backup und Wiederherstellung: Schreibt Backup-Praktiken und Wiederherstellungsvalidierung für Testumgebungen vor.

10.1.6. P18 – Richtlinie zu kryptografischen Kontrollen: Legt verbindliche Verschlüsselungsstandards für ruhende Daten und Daten während der Übertragung innerhalb von Testplattformen fest.

10.1.7. P22 – Richtlinie zur Protokollierung und Überwachung: Regelt Transparenz und Anomalieerkennung für Aktivitäten in Testumgebungen.

10.1.8. P30 – Incident-Response-Richtlinie: Definiert Eskalation und Abhilfemaßnahmen für Datenschutzverletzungen oder Vorfälle im Zusammenhang mit Testsystemen.

10.1.9. P33 – Richtlinie zur Audit- und Compliance-Überwachung: Ermöglicht die Validierung der Richtlinieneinhaltung und deren kontinuierliche Sicherstellung.

11. Referenzstandards und Rahmenwerke

11.1. Diese Richtlinie ist an globalen Cybersicherheitsstandards und regulatorischen Rahmenwerken ausgerichtet, die den sicheren Umgang mit Testdaten und den Schutz von Nicht-Produktivumgebungen vorschreiben.

11.2. ISO/IEC 27001:

11.2.1. Klausel 8.1 – Schreibt die sichere Planung und Steuerung von Testdaten und Testumgebungen vor.

11.3. ISO/IEC 27002:2022 – Maßnahmen 8.28–8.29:

11.3.1. Anhang A Maßnahme 8.28 – Sichere Testdaten: Verlangt den Schutz von in Entwicklungs- und Testphasen verwendeten Testdaten durch Anonymisierung, Maskierung oder synthetische Erzeugung.

11.3.2. Anhang A Maßnahme 8.29 – Schutz von Testumgebungen: Verlangt die Trennung von der Produktivumgebung, Zugriffskontrollen und die Härtung der Umgebung für Testsysteme.

11.3.3. Diese Maßnahmen legen Anforderungen für die sichere Verwaltung von während des Testens verwendeten Daten sowie für den Schutz von Nicht-Produktivsystemen vor Missbrauch, Kompromittierung oder Kontaminierung fest.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. SA-11 – Entwicklertests und -bewertung: Legt Erwartungen an sichere, wiederholbare Testverfahren mit angemessenen Datenkontrollen fest.

11.4.2. SC-28 – Schutz ruhender Informationen: Entspricht der Verschlüsselung von in Nicht-Produktivsystemen gespeicherten Testdaten.

11.4.3. SC-32 – Informationsintegrität: Unterstützt Datenvalidierung, die Vermeidung von Beschädigungen sowie Ein- und Ausgabekontrollen während des Testens.

11.5. EU-DSGVO (2016/679):

11.5.1. Artikel 5 – Datenminimierung: Untersagt die nicht erforderliche Nutzung personenbezogener Daten zu Testzwecken.

11.5.2. Artikel 25 – Datenschutz durch Technikgestaltung: Verlangt, dass Datenschutztechniken von Beginn des Entwicklungs- und Testzyklus an angewendet werden.

11.5.3. Artikel 32 – Sicherheit der Verarbeitung: Schreibt Schutzmaßnahmen für Testumgebungen vor, die personenbezogene oder sensitive Daten verarbeiten.

11.6. EU-NIS2-Richtlinie (2022/2555):

11.6.1. Artikel 21(2)(e), (h): Verlangt sichere Softwareentwicklungs- und Testprozesse mit besonderem Schwerpunkt auf dem Schutz vor unbefugtem Zugriff und Datenabfluss.

11.7. EU-DORA (2022/2554):

11.7.1. Artikel 9 – IKT-Systeme und -Protokolle: Verlangt, dass Testprozesse die Resilienz unterstützen und betriebliche Daten vor Kompromittierung oder unbefugter Offenlegung schützen.

11.8. COBIT 2019:

11.8.1. DSS05 – Sicherheitsdienste verwalten: Unterstützt die Durchsetzung von Sicherheitsrichtlinien in allen Umgebungen, einschließlich Nicht-Produktivumgebungen.

11.8.2. BAI07 – Änderungsannahme und -überführung verwalten: Umfasst den formalen Überführungsprozess von Test in Produktion einschließlich Daten- und Umgebungskontrollen.