dsb

datenschutzbeauftragte
kanton zürich

Glossar und Abkürzungen Informationssicherheit

1 Glossar

Begriff	Erläuterung
AGB Auslagerung Informatikleistungen	Allgemeine Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Informationssicherheit bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen. Diese oder ähnliche Bestimmungen sollten Vertragsbestandteil bei der Auslagerung von IT-Dienstleistungen sein.
Anwendungsverantwortliche (AV)	Die AVs sind verantwortlich für den sicheren Betrieb der Anwendung (Verfügbarkeit der Anwendung und der Datensammlung, Integrität und Vertraulichkeit der enthaltenen Daten). Oft sind die AVs auch Datenverantwortliche.
Asymmetrische Verschlüsselung	Die asymmetrische Verschlüsselung ist ein kryptografisches Verfahren, bei dem jede der kommunizierenden Parteien ein Schlüsselpaar besitzt, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht. Der öffentliche Schlüssel ermöglicht es jeder Person, Daten für die Besitzerin oder den Besitzer des privaten Schlüssels zu verschlüsseln, deren oder dessen digitale Signatur zu prüfen oder sie oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es der Besitzerin oder dem Besitzer, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Vgl. symmetrische Verschlüsselung.
Auftraggebende/r	Auftraggebende/r ist das öffentliche Organ, das einem Dritten, der oder dem Auftragnehmenden, das Bearbeiten von Informationen überträgt.
Auftragnehmende/r	Auftragnehmende sind öffentliche Organe oder private natürliche oder juristische Personen, die Informationen für die oder den Auftraggebende/n bearbeiten. Der Begriff wird als Synonym für Dienstleistende/r bzw. Leistungserbringende/r verwendet.

Authentifizierung	Unter einer Authentifizierung versteht man die Prüfung einer Authentisierung. Dies erfolgt in der Regel durch einen speziellen Authentifizierungsserver, z.B. Active Directory.
Authentisierung	Unter einer Authentisierung versteht man die Vorlage eines Nachweises einer Person, dass sie tatsächlich diejenige ist, die sie vorgibt zu sein. Eine Authentisierung kann unter anderem durch Passworteingabe, Chipkarte oder Biometrie erfolgen.
Authentizität (engl. authenticity)	Die Authentizität ist das Resultat der Authentisierung und der Authentifizierung. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn Personen identifiziert wurden, sondern bezieht sich auch auf IT-Komponenten oder Anwendungen.
Autorisierung (engl. authorization)	Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.
Awareness Training	Vgl. Sensibilisierung
Baustein	Die Bausteine bilden den Kern der IT-Grundschutzkataloge des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Darin werden die Gefährdungen, denen ein Objekt ausgesetzt ist, und die Massnahmen, mit denen es gegen diese Gefährdungen geschützt werden kann, erschlossen.
Basis-Sicherheitscheck	Bei einem Basis-Sicherheitscheck wird geprüft, ob die Minimummassnahmen umgesetzt wurden oder ob Sicherheitsmassnahmen fehlen.
Benutzer-ID	Die Benutzer-ID (Benutzerkennung) dient zur Identifizierung einer Person. Dies kann z.B. ein Benutzername oder eine Vertragsnummer sein.
Browser (engl.)	Mit Browser (von «to browse»; deutsch: schmökern, blättern, umherstreifen) wird die Software zum Zugriff auf das World Wide Web (Internet) bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar. Browser-Produkte sind z.B. Internet Explorer, Firefox, Chrome und Safari.

Bundesamt für die Sicherheit in der Informationstechnik (BSI)	Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) ist Herausgeber des IT-Grundschutzkatalogs.
Client (engl.)	Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzcomputer, der in einem Netz auf Daten und Programme eines Servers zugreift.
Datenschutz-Managementsystem (DSMS)	Ein DSMS ist eine Aufstellung von Verfahren und Regeln innerhalb einer Amtsstelle, die dazu dienen, den Datenschutz und die Informationssicherheit dauerhaft zu gewährleisten.
Datenschutzreview	Mit dem Datenschutzreview kontrolliert die Datenschutzbeauftragte (DSB) die Umsetzung der rechtlichen, organisatorischen und technischen Aspekte von Datenbearbeitungen.
Datenschutzverantwortliche (DSV)	Bei den Datenschutzverantwortlichen handelt es sich um interne Spezialistinnen und Spezialisten, auch Datenschutzberater/innen genannt, die sich um Datenschutzfragen kümmern.
Datenverantwortliche/r (engl. data owner)	Ein/e Datenverantwortliche/r ist für eine bestimmte Datensammlung der Amtsstelle verantwortlich (z.B. Daten des Sozialbereichs). Oft wird diese Rolle der/dem Anwendungsverantwortlichen zugewiesen.
Demilitarisierte Zone (DMZ)	Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. Normalerweise stehen öffentlich zugängliche Server (z.B. Web- und Mailserver) in einer DMZ.
Digitale Signatur	Sicherungsmechanismus für elektronische Daten, bei dem aus der Information mittels eines geheimen Schlüssels ein Wert erzeugt wird, der mit Hilfe eines zugehörigen öffentlichen Schlüssels verifiziert werden kann. Die digitale Signatur dient dem Schutz der Authentizität und der Integrität der Daten. Vgl. auch elektronische Signatur.

Elektronische Signatur	Unter einer elektronischen Signatur versteht man mit elektronischen Informationen verknüpfte Daten, mit denen man die unterzeichnende bzw. signaturerstellende Person identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann.
Empfehlung	Eine Empfehlung ist das Instrument, mit dem die DSB indirekt verbindliche Forderungen anbringen kann. Eine Nichtbefolgung durch das öffentliche Organ kann durch die DSB nach Erlass einer Verfügung durch das betroffene öffentliche Organ auf dem Rechtsweg angefochten werden.
Eskalationsweg	Weg der Meldung bei Störungen oder Angriffen aus dem Netzwerk (von der/dem Auftragnehmenden zur Amtsstelle).
Firewall (engl.)	Eine Firewall (besser mit Sicherheitsgateway bezeichnet) ist ein System aus Soft- und Hardware-Komponenten, um IP-Netze sicher miteinander zu verbinden.
Fortgeschrittene elektronische Signatur (FES)	Die FES ist eine elektronische Signatur, die folgende Anforderungen erfüllt: 1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet. 2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers. 3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann. 4. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.
Gefährdung	Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. So sind beispielsweise Computerviren eine Bedrohung, die zu einer Gefährdung für Anwender/innen werden, wenn wirksame Sicherheitsmassnahmen (Virenscanner) gegen die Bedrohung fehlen und dadurch eine Schwachstelle besteht.

Hacking (engl.)	Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein IT-System einzudringen, seine Schwächen offenzulegen und es gegebenenfalls – bei unethischem Hacking – zu übernehmen.
Hosting	Speichern und Verwalten von Daten bei der oder dem Auftragnehmenden (z.B. Internetauftritt).
Hybride Verschlüsselung	Hybride Verschlüsselung ist ein Verschlüsselungsverfahren, das Methoden der asymmetrischen Verschlüsselung und der symmetrischen Verschlüsselung in geeigneter Weise verknüpft und die Vorteile beider Verfahren verbindet. Heute gängiges Verfahren zur Sicherung der Vertraulichkeit bei elektronischer Kommunikation über offene Netze (z.B. TLS oder IPSec).
Informationssicherheitskonzept	Ein Informationssicherheitskonzept ist ein Plan, mit dem aufgrund der Analyse aller Gegebenheiten mögliche Gefährdungen minimiert bzw. eliminiert werden sollen. Hierzu müssen zuerst die zu schützenden Objekte bestimmt werden. Für diese Objekte sind Schadenszenarien und mögliche Gefährdungen bzw. Bedrohungen zu ermitteln. Unter Beachtung von Eintrittswahrscheinlichkeiten und möglichen Auswirkungen der Gefährdungen werden Massnahmen entwickelt, um den Gefährdungen zu begegnen. Abschliessend sind eine Analyse der Risikotragbarkeit und eine Deklaration der Restrisiken notwendig.
Informationssicherheitsziel (engl. security objective)	Das Informationssicherheitsziel definiert die mit einem Informationssicherheitskonzept zu realisierende Sicherheitsvorgabe (Sollvorgabe). Typische Ziele sind: Authentizität (authenticity), Integrität (integrity), Nichtabstreitbarkeit (non repudiation), Verbindlichkeit (accountability), Verfügbarkeit (availability), Vertraulichkeit (confidentiality) und Zuverlässigkeit (reliability, dependability).
IT-Verantwortliche/r (ITV)	Die oder der ITV ist für den Betrieb der IT-Infrastruktur verantwortlich.

Informatiksicherheitsverordnung ISV (LS 170.8)	Die Informatiksicherheitsverordnung des Kantons Zürich vom 17. Dezember 1997 ergänzt die Bestimmungen des IDG und der IDV und konkretisiert die notwendigen organisatorischen und technischen Massnahmen im Bereich der Informatik.
Informationssicherheit (IS)	Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität etc. sicherstellen. Sie umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.
Informationssicherheits-Managementsystem (ISMS)	Das ISMS ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern und damit auf dem gewünschten Niveau zu halten.
Informationssicherheits-massnahmen	Informationssicherheitsmassnahmen sind Vorkehrungen, die getroffen werden, um ein System gegen Bedrohungen im Bereich der Informationssicherheit zu schützen.
Informationssicherheitsniveau	Die Informationssicherheitsverordnung (ISV) spricht in diesem Zusammenhang von Sicherheitsstufen. Das Informationssicherheitsniveau ist die Zielvorstellung (oder der Zielwert) eines Unternehmens oder einer Behörde bezüglich der Informationssicherheit.
Informationssicherheits-organisation	Die Informationssicherheitsorganisation definiert die zentralen Rollen und Rollentragenden, welche die verschiedenen Aufgaben zur Erreichung der Informationssicherheitsziele wahrnehmen. Dies beinhaltet z.B. die Aufgaben der Gemeindeschreiberin/des Gemeindeschreibers, der oder des Informationssicherheitsverantwortlichen, Datenschutzverantwortlichen und Anwendungsverantwortlichen.

Informationssicherheitsprozess	Ein gesteuerter Sicherheitsprozess (Deming-Kreis: Plan-Do-Check-Act) sichert die umfassende Informations-sicherheit. Die Behörde initiiert diesen Vorgang durch die Übernahme der Verantwortung, die Einrichtung einer geeigneten Informationssicherheitsorganisation und die Delegation von Zuständigkeiten. Das Ergebnis der ersten Phase ist die Leitlinie zur Informationssicherheit, die von der Leitung allen Beschäftigten bekannt gegeben wird. Es folgen die Erarbeitung der Informationssicherheits-ziele und die Analysen zum Ist-Zustand der IT und zur angestrebten Informationssicherheit, die in einem Informationssicherheitskonzept zusammengefasst werden. Fortgesetzt wird der Informationssicherheitsprozess in Phasen der Umsetzung noch fehlender Sicherheits-massnahmen und Massnahmen zur Aufrechterhaltung und Verbesserung der Informationssicherheit.
Informationssicherheits-verantwortliche (ISV)	Die Informationssicherheitsverantwortlichen tragen die Verantwortung für die Umsetzung der Leitlinie zur Infor-mationssicherheit. Sie koordinieren sämtliche Aktivitäten im Bereich der Informationssicherheit.
Integrität (engl. integrity)	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktions-weise von Systemen. Wird der Begriff Integrität auf Daten angewendet, drückt er aus, dass die Daten vollständig und unverändert sind. Der Verlust der Integrität von Informationen kann bedeuten, dass diese unerlaubt verändert, Angaben zur Autorin, zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Integrität ist eine Zielsetzung der Informationssicherheit.
Internet	Globales Computernetz (Netz der Netze), basierend auf dem Übertragungsstandard (Protokoll) TCP/IP. Das Internet funktioniert plattform- und betriebssystemübergreifend. Typische Dienste im Internet sind World Wide Web (WWW) und E-Mail.
Intranet	Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch einen Sicherheits-gateway (Firewall) verhindert oder nur aufgrund spezieller Regeln zugelassen.

Internet Protocol (IP) (engl.)	Verbindungsloses Protokoll der Internet-Schicht im TCP/IP-Referenzmodell. Ein IP-Header enthält in der Version IPv4 u.a. zwei 32-Bit-Nummern (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.
Internet Protocol Version 4 (IPv4)	Das IPv4 ist ein verbindungsloses Protokoll der Vermittlungsschicht und erlaubt den Austausch von Daten zwischen zwei Rechnern. Beispiel einer Adresse: 192.168.1.1.
Internet Protocol Version 6 (IPv6)	Das IPv6 ist die Nachfolgeversion von IPv4 und soll dieses ablösen, da es u.a. die Zahl der verfügbaren Rechneradressen stark erweitert. Beispiel einer Adresse: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344
ISO (engl. International Organisation for Standardization)	Die ISO ist die internationale Vereinigung von Normungsorganisationen. Sie erarbeitet internationale Normen in vielen Bereichen.
ISO 2700x	Reihe von internationalen Normen (der ISO), die sich mit der Erstellung, dem Betrieb und der Steuerung eines Informationssicherheits-Managementsystem (ISMS) befassen.
Informationstechnik (IT)	IT wird vielmals als Synonym für Informationstechnologie verwendet.
IT-Grundschutz	Als IT-Grundschutz bezeichnet man die Standardsicherheitsmassnahmen für typische IT-Objekte (Anwendungen, IT-Systeme, Räumlichkeiten, Netze). Bei einem IT-Grundschutzkonzept wird auf eine detaillierte Risikoanalyse und die differenzierte Einteilung nach Schadenshöhe und Eintrittswahrscheinlichkeit verzichtet. Stattdessen wird von pauschalen Gefährdungen ausgegangen.
IT-Grundschutzkatalog	Der Katalog des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) beschreibt die Gefahren und die zu ergreifenden Massnahmen im Bereich der IT-Sicherheit.
Kennwortchronik	Anzahl der vom System aufbewahrten Passwörter
Klassifizierung	Bei der Klassifizierung wird der Schutzbedarf der Objekte (Assets) definiert. Sie wird vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) als Schutzbedarf und in der Informationssicherheitsverordnung (ISV) als Beurteilung der Negativfolgen bezeichnet.

Kontrolle	Überprüfen des Verhaltens und/oder des Ergebnisses mit dem Ziel der Einwirkung auf das Verhalten (von Menschen, Organisationen oder technischen System). Bei der Kontrolle findet ein Soll/Ist-Vergleich statt.
Kryptografie	Mathematisches Fachgebiet, das sich mit Methoden zum Schutz von Informationen befasst (u.a. mit Vertraulichkeit, Integrität und Authentizität von Daten).
Leitlinie zur Informationssicherheit	Eine Leitlinie zur Informationssicherheit (auch Informationssicherheitsleitlinie, Informationssicherheitspolitik, Informationssicherheitsstrategie) beschreibt den erstrebten Sicherheitsanspruch einer Institution (Behörde, Unternehmen usw.). Die Schwerpunkte liegen im Bereich der elektronischen Datenverarbeitung und den damit einhergehenden Sicherheitsanforderungen. Hierbei liegt die Annahme bzw. Tatsache zugrunde, dass Informationen per se einen Wert darstellen bzw. ihr Schutz per Gesetz oder Verordnung gefordert ist.
LEUnet	Datennetzwerk des Kantons Zürich für die Gemeinden und die kantonale Verwaltung. Das LEUnet ist in logische Netze (z.B. Gemeinden, Spitäler, Kanton usw.) unterteilt.
Log Files	Protokollaufzeichnungen, respektive Protokolldateien. Vgl. Logging
Logging	Schreiben einer Protokolldatei (Log Files), in der Ereignisse wie Zugriffe auf Daten während einer Programmausführung nach bestimmten Regeln festgehalten werden.
Makro	Befehlsfolge oder kurzes Programm zur Vereinfachung für häufig benötigte Aufgaben.
Malware	Der Begriff Malware steht für MALicious SoftWARE – also bösartige Software. Malware dient als Oberbegriff für die Gesamtheit von Schadsoftware. Viren, Würmer, Trojaner, Adware und Spyware sind zum Beispiel Unterkategorien von Malware.
Massnahmenkatalog	Extrakt aus den BSI-Grundschutzmassnahmen. Die Massnahmen sind in zwei Kataloge gegliedert: Minimummassnahmenkatalog und Massnahmenkatalog.

Mobile Datenträger	Dieser Begriff fasst alle Datenträger zusammen, die mit einem Client oder Server Daten austauschen können. Vgl. USB-Stick und -Disk, Smartphone etc.
Modem	Meistens benötigt für die Datenübermittlung über eine Telefonleitung.
mTAN (Mobile TAN)	Die Variante mTAN oder smsTAN besteht aus der Einbindung des Übertragungskanals SMS. Dabei wird die Transaktionsnummer (TAN) per SMS auf ein Mobiltelefon gesendet. Dies wird z.B. zur starken Authentifizierung verwendet.
Network Address Translation (NAT)	Network Address Translation (NAT) bezeichnet ein Verfahren für das automatische und transparente Ersetzen von Adressinformationen in Datenpaketen. NAT-Verfahren kommen meist auf Routern und Sicherheitsgateways zum Einsatz, vor allem um den beschränkten IPv4-Adressraum möglichst effizient zu nutzen und um lokale IP-Adressen gegenüber öffentlichen Netzen zu verbergen.
Network Security Policy	Strategie und Grundregeln im Netzwerkbereich (wie zum Beispiel im LEUnet).
Nichtabstreitbarkeit (engl. non repudiation)	Hier liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen der Nichtabstreitbarkeit der Herkunft (die Absenderin/der Absender soll das Versenden einer Nachricht nachträglich nicht bestreiten können) und der Nichtabstreitbarkeit des Erhalts (die Empfängerin/der Empfänger soll den Erhalt einer Nachricht nachträglich nicht bestreiten können).
Online-Schalter	Der Online-Schalter ermöglicht in Web-Anwendungen eine direkte Eingabe von Daten in Formulare zuhanden der Amtsstelle oder Behörde.
OWA	Der Outlook Web Access (OWA) ist eine von Microsoft verwendete Technik für den Zugriff auf ein E-Mail-Postfach über das Internet.

Patch	Ein Patch (von «to patch»; deutsch: flicken) ist ein kleines Programm, das Software-Fehler wie z.B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.
Penetrationstest	Ein Penetrationstest ist ein gezielter Angriffsversuch auf ein IT-System. Er wird zur Wirksamkeitsprüfung der Sicherheitsmassnahmen eingesetzt.
Phishing (engl.)	Phishing werden Versuche genannt, über gefälschte WWW-Seiten an Daten einer Internetnutzerin, eines Internetnutzers zu gelangen. Oft werden mit Phishing Passwörter ausgespäht.
Public Key Infrastructure (PKI) (engl.)	Der PKI ist eine Sicherheitsinfrastruktur zum verschlüsselten Austausch von Daten und zur Erstellung und Prüfung von Signaturen mit von einer vertrauenswürdigen Stelle ausgegebenen Schlüsselpaaren. Vgl. asymmetrische Verschlüsselung
Privacy Policy (engl.)	Eine Privacy Policy (auch Datenschutzrichtlinie oder Datenschutzerklärung genannt) umschreibt die Massnahmen einer Amtsstelle zur Wahrung der Privatsphäre der Benutzenden. Sie wird oft in den Webauftritt integriert.
Protokoll	Gemeint ist das Protokoll betreffend den Übertragungsstandard und damit die definierte Vereinbarung über die Art und Weise des Informationsaustauschs zwischen zwei Systemen. Damit sind alle Regeln, Formate, Parameter und Eigenschaften gemeint, die zu einer vollständigen, fehlerfreien und effektiven Datenübertragung beitragen.
Proxy (engl.)	Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.
Qualifizierte elektronische Signatur	Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit nach Art. 6 Abs. 1 und 2 Bundesgesetz über die elektronische Signatur (ZertES) und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht.

Remote Access Service (RAS)	Zugriff über Internet und LEUnet auf das lokale Netz oder eine Anwendung der Amtsstelle. Dieser wird meistens von IT-Dienstleistenden und externen Mitarbeitenden genutzt.
Revision	Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-)Richtlinien. Eine Revision sollte unabhängig und neutral sein. Sie ist gemäss § 17 Informationssicherheitsverordnung (ISV) für Amtsstellen Pflicht.
Risikoanalyse	Mit einer Risikoanalyse wird untersucht, wie wahrscheinlich das Eintreten eines schädigenden Ereignisses ist und welche negativen Folgen daraus entstehen.
Rolle (im Rollen- und Berechtigungskonzept)	Eine Benutzerrolle (oder kurz Rolle) definiert Aufgaben und Eigenschaften eines bestimmten Tätigkeitsfeldes (wie zum Beispiel die Rolle als Administrator/in, als Vorgesetzte/r, als Revisor/in etc.).
Rollen- und Berechtigungskonzept (RBK)	Das RBK beschreibt die Rolle und Berechtigungen, die beim Zugriffsschutz verwendet werden. Es beschreibt die Berechtigungs-, Passwort- und Kontrollprozesse.
Router (engl.)	Ein (IP-)Router ist ein Vermittlungsrechner, der Netze auf IP-Ebene koppelt und Wegewahlentscheidungen anhand von IP-Protokollschicht-Informationen trifft. Router trennen Netze auf der Netzzugangsschicht.
Rivest, Shamir, Adleman Public Key Encryption (RSA) (engl.)	Ein sehr verbreitetes, asymmetrisches Verfahren (Public-Key-Verfahren) zur Verschlüsselung und Signaturerstellung.
Schadfunktion	Mit Schadfunktion wird eine von der Anwenderin oder dem Anwender ungewünschte Funktion bezeichnet, die die Verfügbarkeit von Daten, Ressourcen oder Dienstleistungen, die Vertraulichkeit von Daten oder die Integrität von Daten unbeabsichtigt oder bewusst gesteuert gefährden kann.
Schlüsselzertifikat	Ein Schlüsselzertifikat ist eine digitale Unterschrift (Signatur) eines öffentlichen Schlüssels, um die Authentizität einer Kommunikationspartnerin/eines Kommunikationspartners zu verifizieren. Anwendungsbereiche sind z.B. die Verschlüsselung von E-Mails und Webseiten.

Schutzbedarf (engl. protection requirements)	Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik angemessen ist. Sinnvollerweise wird der Schutzbedarf pro Informationssicherheitsziel und Informationsobjekt definiert.
Schwachstelle (engl. vulnerability)	Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Durch eine Schwachstelle wird eine Bedrohung zur Gefährdung, ein Objekt also anfällig für Bedrohungen.
Secure Sockets Layer (SSL)	Protokoll zur sicheren Kommunikation über das Internet, insbesondere zwischen Client und Server, basierend auf dem Verschlüsselungsalgorithmus RSA, z.B. eingesetzt zur Verschlüsselung von Webseiten (https). Mittlerweile abgelöst durch Transport Layer Security (TLS).
Sensibilisierung	Sensibilisierung bezeichnet im Zusammenhang der Informationssicherheit die Bildung von sogenannter IT Security Awareness, also die Schärfung des Bewusstseins der Mitarbeitenden für Sicherheitsprobleme (-risiken).
Server (engl.)	Als Server wird Soft- oder Hardware bezeichnet, die Anderen (Clients) bestimmte Dienste anbietet. Typischerweise wird damit ein Computer bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Computern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- und E-Mail-Server.
Sicherheitsgateway	Ein Sicherheitsgateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen (z.B. LEUnet und internes Netz). Dies bedeutet, dass ausschliesslich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.
Sicherheitsstufe S1-3	Die Informationssicherheitsverordnung (ISV) definiert 3 Sicherheitsstufen (S1 bis S3). Die Amtsstellen sind verpflichtet, die angemessene Sicherheitsstufe zu definieren.

Signatur	Vgl. digitale Signatur, vgl. elektronische Signatur, vgl. fortgeschrittene digitale Signatur, vgl. qualifizierte digitale Signatur.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches Mobiltelefon zur Verfügung stellt. Aktuelle Smartphones lassen sich meist über zusätzliche Programme (sogenannte Apps) von der Anwenderin/dem Anwender individuell mit neuen Funktionen aufrüsten.
Spoofing (engl.)	Spoofing (von «to spoof», deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.
Symmetrische Verschlüsselung	Verschlüsselung, bei der Informationen mit demselben Schlüssel ver- und entschlüsselt werden. Der Schlüssel muss dabei über einen sicheren Kanal übertragen werden. Vgl. asymmetrische Verschlüsselung
Transaktionsnummer (TAN)	Geheimzahl, die die Freigabe für einen einzelnen Vorgang erteilt und danach ihre Gültigkeit verliert. Wird insbesondere beim Internet Banking in Kombination mit einer PIN eingesetzt. Vgl. mTAN (Mobile TAN)
Transport Layer Security (TLS)	Protokoll zur sicheren Kommunikation über das Internet, insbesondere zwischen Client und Server, basierend auf dem Verschlüsselungsalgorithmus RSA, z.B. eingesetzt zur Verschlüsselung von Webseiten (https). Nachfolgebezeichnung für Secure Sockets Layer (SSL)
Uniform Resource Locator (URL)	Adressierungsschema für Dokumente und sonstige Dateien im Internet, bestehend aus Protokoll und Adresse. Beispiel einer Adresse: https://www.datenschutz.ch.
USB-Stick und -Disk	USB ist eine universelle Schnittstelle zum Anschluss von Geräten an Server und Clients, USB-Sticks und -Disks sind Typen von Datenträgern, die sich über diese Schnittstelle anschliessen lassen.

Verbindlichkeit (engl. accountability)	Unter Verbindlichkeit werden die Informationssicherheits-ziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.
Verfügbarkeit (engl. availability)	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzer/innen stets wie gewünscht zur Verfügung stehen. Verfügbarkeit ist eine Zielsetzung der Informations-sicherheit.
Verschlüsselung (engl. encryption)	Verschlüsselung (Chiffrieren) transformiert einen lesbaren Klartext (oder auch Informationen anderer Art, wie Ton- oder Bildaufzeichnungen) in Abhängigkeit von einer Zusatzinformation, die Schlüssel genannt wird, in einen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation – die Zurückgewinnung des Klartexts aus dem Geheimtext – wird Entschlüsselung genannt.
Vertraulichkeit (engl. confidentiality)	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschliesslich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist eine Zielsetzung der IT-Sicherheit.
Virtual Private Network (VPN)	Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft dem Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner und -partnerinnen sicher authentisiert werden, auch dann, wenn mehrere Netze oder Computer über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.
Wert (engl. asset)	Werte sind in der Informationssicherheit Elemente, die geschützt werden müssen. Dies können z.B. Personendaten, Anwendungen, IT-Systeme, Räume usw. sein.
Wireless Local Area Network (WLAN)	Wireless LAN, deutsch: drahtlose lokale Netzwerke, lokale Funknetzwerke

Zertifikat	Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem das IT-Grundschutz-Zertifikat, Schlüsselzertifikate, IT-Sicherheitszertifikate (z.B. auf Basis von ISO 27001 oder das Datenschutz-Managementsystem (DSMS)-Zertifikat nach § 13 IDG) und Common-Criteria-Zertifikate.

2 Abkürzungsverzeichnis

Abkürzung	Begriff
AV	Anwendungsverantwortliche / -verantwortlicher
BSI	Bundesamt für die Sicherheit in der Informationstechnik (Deutschland)
DMZ	Demilitarisierte Zone
DSB	Datenschutzbeauftragte des Kantons Zürich
DSMS	Datenschutz-Managementsystem
FES	Fortgeschrittene elektronische Signatur
GS	Grundschutz
IDG	Gesetz über die Information und den Datenschutz (LS 170.4)
IDV	Verordnung über die Information und den Datenschutz (LS 170.41)
IT	Informations- und Kommunikationstechnologie
IP	Internet Protokoll
IS	Informationssicherheit
ISMS	Informationssicherheits-Managementsystem
ISO	International Organisation for Standardization
ISV	Informationssicherheitsverantwortliche / -sicherheitsverantwortlicher
ISV (Verordnung)	Informatiksicherheitsverordnung (LS 170.8)
IT	Informationstechnik
ITV	IT-Verantwortliche / -Verantwortlicher
LAN	Local Area Network
NAT	Network Address Translation
OWA	Outlook Web Access

PKI	Public Key Infrastructure
RAS	Remote Access Service
RBK	Rollen- und Berechtigungskonzept
RSA	Rivest, Shamir, Adleman Public Key Encryption
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TAN	Transaktionsnummer
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

V 5.1 / November 2019

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh