Zusätzliche Vertragsbedingungen – Informationssicherheit

1. Allgemeines, Zweck und Geltungsbereich

Dieses Dokument beschreibt die zusätzlichen Bedingungen der **Leipziger Wasserwerke (LWW)** an die Informationssicherheit für vertraglich gebundene Lieferanten und Dienstleister, nachfolgend **Auftragnehmer (AN)** genannt.

1.1. Der Auftragnehmer **(AN)** benennt vor Beginn seiner Tätigkeit schriftlich einen Verantwortlichen, der die Einhaltung und Durchsetzung der vertraglichen Anforderungen beim **AN** und ggf. dessen **SUB**-Unternehmen **(SUB)** veranlasst und/oder überprüft. Er muss insbesondere die Einhaltung der nachfolgenden Informationssicherheitsanforderungen überwachen und bei Mängeln geeignete Gegenmaßnahmen zu deren Beseitigung ergreifen.

1.2. Dem Verantwortlichen des **AN** obliegt die Verpflichtung, sich zu Beginn der Leistungserbringung in die **Meldewege** der LWW einweisen zu lassen. Dieser Verantwortliche hat nach der Einweisung dafür zu sorgen, dass der **AN**, als auch gebundene **SUB**-Unternehmen, alle festgestellte Sicherheitsereignisse, Informationssicherheitsvorfälle und Schwachstellen unverzüglich entsprechend bekannter Meldewege **(°)** der LWW gemeldet werden. Die Erkennung von Sicherheitsereignissen und -vorfällen sowie die Meldewegesind Anhang 3 zu entnehmen.

1.3. Der **AN** meldet den LWW **Abweichungen** von den vereinbarten Lieferantenprozessen und Maßnahmen im Zusammenhang mit dem Vertrag. Die LWW sind berechtigt, in regelmäßigen Abständen diese Lieferantenprozesse und Maßnahmen zu überprüfen. Um **Lieferantenaudits** durchzuführen, gewährt der **AN** Zugang zu vertraglich vereinbarten Informationen und zu seinen relevanten Unternehmensteilen.

1.4. Der **AN** muss sicherstellen, dass der **SUB** die ihm übertragenen Leistungen nicht weiter vergibt. Es sei denn, die LWW hat dies zuvor schriftlich genehmigt.

1.5. Liefert der **AN** Technologie-Produkte, verpflichtet er auch alle Lieferanten der Lieferkette auf die vereinbarten **Sicherheitsanforderungen** und **-praktiken**. Das Gleiche gilt für Leistungen einschließlich des Einsatzes von **SUB** in der Leistungserbringung.

1.6. Sofern der **Lebenszyklus** von Komponenten der Informations- und Kommunikationstechnologie in Kürze endet oder diese generell nicht mehr zur Verfügung stehen werden, wird der **AN** die LWW über die daraus entstehenden Risiken informieren sowie den verbleibenden end-of-support[1] (EoS bzw. end-of-support, insbesondere security) Zeitraum anzeigen

1.7. Auf Verlangen weist der **AN** die Herkunft der beauftragten Komponenten nach, deren Ausfall oder Fehlen eine Erhöhung des Informationssicherheitsrisikos zur Folge hat. Der AN unterstützt die LWW bei einer entsprechenden Überprüfung der Lieferkette.

1.8. Der **AN**, der Zutritt (siehe Sicherheitszone) zu Standorten der Leipziger Wasserwerke (LWW) und/oder Zugriff auf LWW-Informationen (siehe Vertraulichkeitsklassifizierung) hat, ist zur Verschwiegenheit verpflichtet.

1.9. Foto-, Audio- und Videoaufnahmen sowie deren Veröffentlichung sind zu genehmigen. Inhalte, die nicht fotografiert oder aufgenommen werden dürfen, sowie die Rahmenbedingungen für die Veröffentlichung von Aufnahmen sind dem Anhang 1 „Einschränkungen und Ausschlusskriterien für Audio-, Video- und Fotoaufnahmen“ zu entnehmen. Sollte der AN oder einer seiner SUBs Aufnahmen im Eigeninteresse planen, so ist er verpflichtet die „Vereinbarung zur Erstellung und Nutzung von Audio-, Video- und Fotoaufnahmen durch Dritte“ auszufüllen und von der LWW freigegeben zu lassen. In dem Fall wenden Sie sich bitte an ihren Vertragspartner der LWW.

1.10. Sollten digitale Konferenzsysteme zur Anwendung kommen werden, ist Anhang 2 zu beachten.

1.11. Verfügt der **AN** über Zertifizierungen nach ISO/IEC 27001:2013 oder gleichwertig, z.B. IT-Grundschutz, oder höherwertige Zertifizierungen, z.B. PCI-DSS, sind diese den LWW nachzuweisen.

1.12. Nach ISO/ IEC 27001:2013, gleichwertig oder höherwertig zertifizierte **AN** hat der LWW auf Verlagen einen aktuellen Schulungsnachweis (nicht älter als 12 Monate ab Auftragsdatum) zu übermitteln.

2. Physische Sicherheit

2.1 Die **Hausordnungen** sind einzuhalten.

2.2 Mitarbeiter des **AN** und seiner **SUB** haben zu Räumen und Einrichtungen der LWW nur **Zutritt**, soweit sie für diese ausdrücklich autorisiert wurden.

2.3. Sie tragen auf den Betriebsgeländen der LWW sichtbar die **Besucherausweise**.

2.4 Der physische Zutritt bei kritischen Standorten ist grundsätzlich auf vereinbarte Sicherheitszonen beschränkt. Der **AN** muss eine aktuelle Liste des Personals mit Zutrittsberechtigung in Koordination mit den jeweiligen Standortverantwortlichen der LWW pflegen und vorhalten. Hierfür eigens ausgestellte Ausweise/Zugangskarten sind personalisiert und nicht übertragbar.

2.5. Standortspezifische Regelungen zur Zutrittskontrolle sind einzuhalten.

2.6. Bei der Planung neuer Technik- bzw. Serverräume muss die „DIN EN 50600 Reihe" berücksichtigt, geprüft und in Angemessenheit angewandt und projektiert werden.

2.7. Bei der Planung eines neuen Rechenzentrums müssen die Anforderungen der „DIN EN 50600 Reihe" berücksichtigt bzw. projektiert werden.

3. IT-/OT-Zugangssteuerung und Umgang mit Zugangsdaten

3.1 Zugänge und Zugriffe innerhalb des internen Netzwerkes werden durch die LWW berechtigt und protokolliert.

3.2. Wenn zur Dienstleistungserbringung Fernzugänge zu IT-/OT-Systemen und Anwendungen der LWW (auch bei weiterführenden RDP-Verbindungen) notwendig werden, ist ein Zugang zu den Systemen ausschließlich über das LWW Remote Access Portal (https://secureportal.wasser-leipzig.de/) sicher zu stellen bzw. dieses zu bevorzugen. Ausnahmen davon sind von den LWW zu genehmigen.

3.3. Fernzugriffe sind für einen eingeschränkten Personenkreis des **AN** und seiner **SUB** im Vorfeld zu beantragen.

3.4. Änderungen an den bei der LWW berechtigten Benutzern des **AN** sind den LWW anzuzeigen **(*).** Die Benennung neuer Benutzer für den **AN** hat in einem gesonderten Antragsformular zu erfolgen. Scheidet ein Mitarbeiter des **AN** aus dem Unternehmen aus, der Berechtigungen bei der LWW hat, ist dies unverzüglich anzuzeigen.

3.5 Jeder Mitarbeiter des **AN** und seiner **SUB** hat sichere Passwörter zu generieren/zu verwenden (mindestens 10 Zeichen unter Verwendung von Groß- und Kleinbuchstaben, Zahlen, ggf. Sonderzeichen und kontextfrei). Für eine Anmeldung sind sichere Passwörter zu verwenden (weiterführende Informationen gemäß der BSI-Internetseite „BSI - Sichere Passwörter erstellen (bund.de)". Diese Passwörter dürfen nicht weitergegeben werden.

3.6. Die Zusendung eines automatisch generierten Passwortes erfolgt in einer separaten Mitteilung. Ggf. automatisch generierte Initialpasswörter müssen bei der ersten Anmeldung zwingend geändert werden.

3.7. Die Weitergabe überlassener Zugangsdaten (Benutzer/Passwort/weiterer Faktoren) ist untersagt.

3.8. Der Mitarbeiter des **AN** und oder des **SUB** haben dafür Sorge zu tragen, dass ihre Zugangsdaten nicht durch Dritte einsehbar, nicht im Klartext gespeichert, beispielsweise in Textdateien oder in Internetbrowsern (Funktion „Passwort speichern"), ordnungsgemäß verwaltet, z.B. in einem Passwortmanager, sind sowie für berufliche und private Zwecke nicht die gleichen Passwörter verwendet werden.

3.9. Sollte der Benutzer des **AN** Kenntnis darüber erlangen, dass seine Zugangsdaten (Passwort/privater Schlüssel/weiterer Faktor etc.) einem Dritten bekannt geworden sein könnten, hat der Nutzer dieses unverzüglich bei der LWW anzuzeigen*****. In dem Fall ist sofort nach Bekanntwerden das Passwort/Schlüsselpaar zu wechseln.

3.10. Soweit ein Mitarbeiter des **AN** aktive Sitzungen (z. B. Cloud-Anwendungen, Netzwerkdienste und Anwendungen) nicht mehr benötigt, meldet er diese unverzüglich ab.

4. Netzwerk- und Fernzugänge auf die LWW IT-/OT-Infrastruktur sind dem AN nur unter folgenden Maßgaben gestattet:

4.1. Es gelten die unter 3. aufgeführten Regelungen für den sicheren Umgang mit Zugangsdaten.
4.2. Die Mehrfaktorauthentifizierung ist einzurichten. Ein Ausschluss der Nutzung des Mehrfaktorauthentifizierungssystems ist vor Erstzugang von den LWW zu genehmigen und vom **AN** bzw. seiner **SUB** zu begründen und zu dokumentieren.
4.3. Die Einwahl erfolgt nur bei Bedarf und in Abstimmung mit der IT/OT der LWW. Der Gültigkeitszeitraum der Einwahl ist auf die Vertragslaufzeit beschränkt. Der Umfang der Einwahl ist auf den Vertragsgegenstand eingeschränkt.
4.4. Das vom **AN** zur Einwahl genutzte System, wenn nicht durch die LWW gestellt, muss über eine aktuelle Schutzsoftware vor Malware (z.B. Endpoint Protection) verfügen und durch aktuellste Virenpattern und -signaturen geschützt sein.
4.5. Das vom **AN** zur Einwahl genutzte System, wenn nicht durch LWW gestellt, muss über den aktuellsten Stand von Sicherheitspatchen verfügen.
4.6. Die vom **AN** genutzte VPN-Verbindung (z. B. in Projektphase), wenn nicht durch die LWW gestellt, muss nach dem Stand der Technik gesichert sein. Die LWW behalten sich vor, dem **AN** die Verwendung von Kryptographie-Lösungen (Mindeststandard) vorzuschreiben.
4.7. Die Verwendung von veralteten (**Nicht** Stand der Technik) und als unsicher bekannten Kryptographiestandards durch den **AN** ist untersagt. Als aktueller Stand der Technik gilt die Empfehlung des BSI entsprechend der Technischen Richtlinie des BSI „TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen".
4.8. Inselnetzwerke (black Box Netzwerke) des **AN** sind technologisch zu vermeiden und unterliegen vor Inbetriebnahme der Zustimmung durch die LWW. Sie dürfen ohne vorherige Genehmigung der LWW keine Verbindung zu Netzwerksegmenten, insbesondere zum Produktionsnetzwerksegment, herstellen.
4.9. Sind Inselnetzwerke nicht zu vermeiden, ist das von ihnen ausgehende Risiko (unkontrollierter Zugang) für die LWW im Rahmen einer Risikoanalyse zu bewerten und, nach Möglichkeit, nach Dienstleistungserbringung bzw. Beendigung des Auftrages wieder zu entfernen. Der AN bzw. SUB hat die LWW bei der Risikoanalyse zu unterstützen.

4.10. Der Fernzugang und -zugriff auf informationsverarbeitende Systeme in verfahrenstechnischen Anlagen der Prozessdaten- und Steuerungsdatenverarbeitung (PDV) ist ab der Inbetriebnahme nur noch durch die von den LWW bereitgestellten Fernzugangstechnologien (Zugänge, z.B. temporär gestellte remote-Verbindung) möglich. Begründete Ausnahmen (vom **AN** bzw. **SUB** eingesetzte Fernzugangstechnologien) sind von den LWW zu genehmigen.
4.11. Notwendige Protokollierungen (Funktionalitätsnachweis während der Inbetriebnahme und/oder Abnahme) sind durch die von den LWW bereitgestellte Software nachzuweisen. Eventuelle Ausnahmen davon sind von den LWW zu genehmigen.
4.12. Der **AN** verpflichtet sich, die LWW Netzwerk- und Zugangsüberwachung zuzulassen.
4.13. Nicht benötigte Netzwerkzugänge (TCP/IP- oder UDP-Ports) müssen im Standard deaktiviert sein. Abweichungen müssen von den LWW freigegeben werden.

5. Umgang mit Hard- und Software

5.1. Im internen IT-Netz der LWW dürfen nur von LWW genehmigte IT-Komponenten installiert und eingesetzt werden.

5.2. Die Anwendung des Schwachstellen- und Patch-Managementprozesses nach LWW oder AN-Vorgaben sind zu vereinbaren.

5.3. Der **AN** hat jede Software oder Softwarekomponente, die vertraglich vereinbart wurden ist sowie jede Softwarewarekomponente von Drittanbietern (z.B. Datenbanken, Webserver, Schnittstellen, Laufzeitumgebungen etc.), die für einen funktionstüchtigen Betrieb der Software oder ihrer Komponenten notwendig sind, zu installieren oder bereit zu stellen, mit aktuellen Security-Patches zu versorgen sowie diese, nach Freigabe durch die LWW, auf aktuellem Security-Patchstand zu halten. Jedwede andere Software, die nicht Teil der vertraglichen Leistung ist, darf nicht ohne vorherige Freigabe durch die LWW installiert werden.

5.4. Die Anwendung des Change- und Projekt-Managementprozesses nach LWW oder AN-Vorgaben sind zu vereinbaren.

5.5. Der **AN** hat jede Änderung der Software oder Änderung der Softwarekomponente, die vertraglich vereinbart wurden ist sowie jede Änderung der Softwarewarekomponente von Drittanbietern, die für einen funktionstüchtigen Betrieb der Software oder ihrer Komponenten notwendig, nach Freigabe durch die LWW, umzusetzen oder mitzuwirken. Jedwede Änderung an andere Software, die nicht Teil der vertraglichen Leistung ist, darf nicht ohne vorherige Freigabe durch die LWW installiert werden.

5.6. Änderungen an sicherheitsrelevanten Systemen und Anwendungen, Diensten, Einstellungen und Konfigurationen (z. B. Sicherheitssysteme, Firewall, OT Komponenten etc.) oder sind **allein der LWW vorbehalten oder** im Rahmen der Dienstleistungserbringung **von LWW zu genehmigen**. Insbesondere das Deaktivieren dieser Applikationen, Dienste oder das Abschalten automatischer Updates ist **untersagt**.

5.7. Temporäre Außerbetriebnahmen oder vergleichbare Anforderungen zur Dienstleistungserbringung sind der LWW anzuzeigen.

5.8. Sollten IT-/OT-Systeme oder einzelne IT/OT-Komponenten über Funktionen zur Fernwartung verfügen und sollen diese nicht verwendet werden, sind diese zu deaktivieren.

5.9. Von der LWW vorgegebene Konfigurationsstandards und Sicherheitsvorschriften sind vom **AN** einzuhalten. Abweichungen müssen von der LWW freigegeben werden.

5.10. Der **AN** stellt sicher, dass seine Lösung frei von „Back-doors“ ist, die Sicherheitsmechanismen nach dem Stand der Technik umgehen könnten.

5.11. Es sind die vorhandenen Standards der sicheren Softwarearchitektur bei der System- und Softwareentwicklung anzuwenden. Dabei ist der Softwareentwicklungsprozess gemäß des *Security by Design* Prinzips auszulegen.

5.12. Zu implementierende Sicherheitsmaßnahmen für Clouddienste haben sich am aktuellsten Stand der Technik nach ISO/IEC 27017 oder dem Cloud Computing Compliance Criteria Catalogue (C5) des BSI zu orientieren und sind im Bedarfsfall anzupassen.

5.13. Die außerhalb der beauftragten Leistung liegende Nutzung der bereitgestellten Infrastruktur sowie das Überwinden von Schutzmaßnahmen sind untersagt.

5.14. Dem AN ist es untersagt, Hard- oder Softwareprodukte der LWW im Wege des sog. „Reverse Engineering“ zu beobachten, zu untersuchen, zu dekompilieren, rückzubauen oder zu testen.

5.15. Der **AN** hat für einen geplanten oder beauftragten Betrieb oder Nutzung von Cloudapplikationen und -services als auch extern angebundener Cloudapplikationen und -services die LWW Cloud-Checkliste auszufüllen und im Vorfeld zu übermitteln.

5.16. Der **AN** hat für einen geplanten oder beauftragten Betrieb oder Nutzung von Cloudapplikationen und -services als auch extern angebundene Nutzung von Cloudapplikationen und -services ein technisches Schaubild (z.B. ein Netzwerkplan) oder ein Schaubild zu übermitteln, dass die Kommunikationsbeziehungen mit den eingesetzten Protokollen und Ports als auch den Übertragungsrichtungen darstellt.

5.17. Bei Bedarf hat der **AN** der LWW das Sicherheitskonzept oder die Sicherheitsbetrachtung seiner Applikation zu übermitteln.

5.18. Der Zugang und Zugriff vor Ort auf informationsverarbeitende Systeme in verfahrenstechnischen Anlagen der Prozessdaten- und Steuerungsdatenverarbeitung (PDV) ist ab der Inbetriebnahme nur noch durch die von den LWW bereitgestellten Technologien (Hardware und Software, z.B. gestellte Servicenotebooks oder gestellte Servicenotebooks mit DL-VM‘s) möglich. Begründete Ausnahmen (vom **AN** bzw. **SUB** eingesetzte Fernzugangstechnologien) sind von den LWW zu genehmigen.
5.19. Computer, Terminals und mobile Endgeräte sind bei Nichtnutzung und Verlassen mit einem Passwort zu sperren.

5.20. Überlassene Arbeitsmittel müssen nach Beendigung der Dienstleistung zurückgegeben werden.

5.21. Beschädigung oder Verlust der dem **AN** überlassenen dienstlichen Geräte ist unverzüglich zu melden (*****).

5.22. Eine Weitergabe von an den **AN** überlassenen dienstlichen Geräten an unautorisierte Dritte ist untersagt.

5.21. Sofern der **AN** einen nicht aktuellen Stand der Sicherheitsupdates des Betriebssystems und/oder der installierten Software auf dem überlassenen Gerät feststellt, ist er verpflichtet die LWW (*****) vor Beginn der Arbeiten zu informieren.

5.22. Die Nutzung von Wechselmedien (z. B. USB-Sticks, externen Festplatten, SD-Karten), die nicht von den LWW ausgegeben wurden, ist untersagt. Ausnahmen genehmigt die LWW (*****) durch ausdrückliche Einwilligung in begründeten Einzelfällen.
5.23. Es darf nur Software mit Lizenzen für juristische Personen eingesetzt werden. Ein Lizenzmanagement über Lizenzserver ist anzustreben.

6. Umgang mit Informationen, Informationsaustausch,-übertragung und -bereitstellung

6.1. Durch den **AN** erstellte oder bearbeitete Dokumente sind mindestens als „zur internen Verwendung" zu kennzeichnen sowie entsprechend der Kennzeichnung zu behandeln. Über die Art der Kennzeichnung und Klassifizierung hat sich der **AN** bei LWW vor Leistungserbringung zu informieren. Es ist vom **AN** sicher zu stellen, dass nur die auf dem Dokument bezeichnete Zielgruppe, z.B. der Vertragspartner, Kenntnis und Umgang mit den Informationen hat.
6.2. Vertrauliche oder geheime Informationen sind verschlüsselt zu übertragen.
6.3. Für einen Informations- und Datenaustausch sind prioritär LWW Applikation und Dienste, z.B. Large File Management, Managed File Transfer, docserv, Sharepoint etc. zu verwenden.

6.4. Frei verfügbare Dienste, z. B. dropbox, We-transfer oder vergleichbare Services, sind für einen Informations- und Datenaustausch nicht erlaubt.
6.5. Der **AN** ist, auch nach der Verwendung/Dienstleistungserbringung, verpflichtet, erlangte Informationen zu schützen sowie angemessen damit umzugehen.

6.6. Die Bereitstellung von Informationen in öffentlichen Netzwerken, z. B. bei Betrieb eines Webservers, muss mit einer Verschlüsselung nach aktuellem Stand der Technik geschützt sein. Vor dem Produktiveinsatz muss jeder Service über den Dienst von SSLLabs (https://www.ssllabs.com/ssltest/) überprüft werden. Das Ergebnis ist per Screenshot zu dokumentieren. Abweichungen vom Ergebnis „A" sind der LWW anzuzeigen. Die Systeme zur Bereitstellung von Informationen in öffentlichen Netzwerken darf erst produktiv genutzt werden, wenn durch entsprechende Änderungen ein „A" als Prüfungsergebnis erreicht wird. Ausnahmen sind ausführlich zu begründen und von den LWW zu genehmigen.
6.7. Datenspeicherung an Standorten bei Cloudanbietern außerhalb der europäischen Union ist nicht erlaubt.

7. Dokumentation

7.1. Der **AN** hat alle Assets in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zum Informationssystem der LWW zwecks Wartung oder Betriebszugang haben können. Er hat den Schutz dieser Information angemessen sicherzustellen und zu dokumentieren.

7.2. Die Festlegungen der technischen Richtlinie zur Softwarestrukturierung für Automatisierungssysteme, des Technischen Regelwerkes E- & MSR-Technik sowie der Materialstandardisierung und -Vorzugsliste E- & MSR Technik sind einzuhalten.

7.3. Der **AN** stellt sicherheitstechnische Informationen, beispielsweise Datenflussschemata, Sicherheitskonzept, Beschreibung zu proprietären Sicherheitsmechanismen, Systemarchitekturen, Softwareliste mit Patchlevel etc., bei Bedarf zur Verfügung.

*** = it.wasserwerke@L.de** oder **0341/9693666**
° = it.wasserwerke@L.de oder **0341/9693666** oder **LWW Intranet/ Self Service Portal/ Informationssicherheitsvorfall melden (Schloss-Symbol)**

Abkürzung:
IT = Informationstechnik (Information Technology)
OT = Operative Technologien (Operational Technology)
PDV = Prozessdaten- und Steuerungsdatenverarbeitung

Definition:
[1] = „**End of Support" (EoS)** werden Systeme bezeichnet, bei denen keine sicherheitskritischen Fehler und Schwachstellen mehr behoben werden.

Anhang 1: „Einschränkungen und Ausschlusskriterien für Audio-, Video- und Fotoaufnahmen“

A) **Einschränkungen vor** Erstellung/Verwendung/Veröffentlichung von Foto-/Audio-/Videoaufnahmen:

Ist eine Erstellung, Verwendung und/oder eine Veröffentlichung von Foto-/Audio-/Videoaufnahmen beabsichtigt, ist diese **vorab** durch die LWW zu genehmigen. Dabei wird durch die LWW festgelegt, ob die Aufnahmen unverändert, eingeschränkt (z.B. verpixelt, mit Unschärfe versehen) werden müssen oder gar nicht aufgenommen und/ oder gar nicht veröffentlicht werden dürfen. Die LWW legt ggf. weitere Einschränkungen (zeitliche Begrenzung, Nutzungsrecht, Metadaten) fest.

B) Sofern es durch die LWW nicht explizit beauftragt wurde, ist die Anfertigung von Foto-/Audio-/Videoaufnahmen mit folgenden Inhalten **ausgeschlossen**:

- Zutrittsteuerung und Sicherheitszonierungen der LWW-Anlagen und Gebäude sowie Lage- und Gebäudepläne (sämtliche Informationen der physischen Sicherheit)
- Anlagentechnik der Sicherheitszone 3 und 4 (Baukörper und Verfahrenstechnik)
- Sicherheitstechnik und Überwachungssysteme (Öffnungserkennung, Innenraumüberwachung, Videoüberwachung, Sicherheitskameras, Brandmeldeanlagen, Einbruchmeldeanlagen, Wachschutz etc.)
- Schaltanlagen, Transformatoren, Frequenzumrichter, Netzersatzaggregate oder USV-Anlagen (Unterbrechungsfreie Stromversorgung) der LWW (sämtliche Anlagen der Strom- oder Notstromversorgung)
- Messcontainer/Online-Überwachungen/Sensoren/Aktoren/Analyse-Equipment etc. der LWW (sämtliche Anlagen für Messungen/Analysen etc.)
- Herstellerangaben, Produktangaben, Softwareversionen, Visualisierungen, Schaltbilder, Netzwerkpläne, Datenleitungen etc. von Elektrotechnik/OT (Automatisierung und E-MSR) sowie IT-Anlagen der LWW (sämtliche elektrotechnische, IT- oder Automatisierungsgeräte oder -software, Pläne oder Infrastrukturkomponenten, wie Datenleitungen etc. der LWW)
- zur Zugangssteuerungen überlassener Zugangsdaten (Passwörter, Token etc.)
- Informationen zu Automatisierungsvorgängen, z.B. Pumpensteuerungen o. Ä. der LWW
- Informationen über Mitarbeiter der KWL-Gruppe, wenn Sie nicht der DS-GVO entsprechen
- Informationen über weitere durch die LWW verpflichtete Lieferanten/Dienstleister

Anhang 2: Sicherheits-Anforderungen im mobilen Arbeiten/Umgang mit digitalen Konferenzsystemen:

A) Generelle Vorgaben:

- Im mobilen Arbeiten gelten dieselben Sicherheitsprinzipien und Regelungen wie auch in der betrieblichen Umgebung bzw. wie in vertraglichen Vereinbarung definiert.
- Im Umgang mit personenbezogenen Daten der LWW müssen die gesetzlichen Anforderungen der DS-GVO eingehalten werden.
- Das Verbinden von privaten smarten Geräten, wie Smart-TVs, Tablets etc., mit von den LWW bereit gestellter Hardware ist untersagt.
- Private, **nicht** smarte Eingabe- und/oder Anzeigegeräte (d.h. Tastatur, Maus und Monitor) dürfen im mobilen Arbeiten verwendet werden.
- Sicherheitsupdates für das Betriebssystem sowie die darauf installierten Anwendungen sind zeitnah zu aktualisieren. Regelung 4.4 und 4.5. sind anzuwenden.
- Die Nutzung von WLAN, das NICHT-kennwortgeschützt ist (z.B. WLAN-Hotspots ohne Passwort), für dienstliche Zwecke, z.B. Videokonferenzen, ist untersagt.
- Öffentliche WLAN-Hotspots dürfen nicht für dienstliche Zwecke genutzt werden. Stattdessen sind die Hot-Spot Funktion oder ev. bereitgestellte Anwendungen des dienstlichen Smartphones zu nutzen.
- Datenübertragung: siehe Regelung 6.3. und 6.4. beachten
- Es ist untersagt, dienstliche Informationen der LWW mit privater Software zu bearbeiten.
- Das Speichern dienstlicher Informationen der LWW auf privaten (Netzwerk-)Speichern oder anderen Speichermedien im privaten lokalen Netzwerk ist untersagt.
- Geräte mit Zugriffsmöglichkeiten ins Firmennetzwerk der LWW (z.B. beim Arbeiten mit dienstlichen Geräten über VPN-Verbindung oder über das zentrale Zugangsportal (https://secureportal.wasser-leipzig.de)) müssen bei Unterbrechung (z. B. Pause) oder Beendigung der Tätigkeit gesperrt werden.
- Meldung von festgestellten Sicherheitsereignisse, Sicherheitsvorfälle und Schwachstellen siehe Regelung 1.2.
- betriebliche Dokumente dürfen ausschließlich in den betrieblichen Standorten der AN, der SUB oder der kommunale Wasserwerke Leipzig GmbH entsorgt werden. Eine Entsorgung über den privaten Hausmüll ist nicht zulässig.
- Nach Arbeitsende müssen alle Unterlagen, welche eine Klassifikation “vertraulich oder persönlich“ oder höher haben, verschlossen bzw. mindestens an einem für Dritte nicht einsehbaren Ort aufbewahrt werden.
- Die Nutzung privater Faxgeräte für den Versand von Dokumenten, welche eine Klassifikation „vertraulich“ oder „persönlich“ oder höher haben, ist untersagt.

B) Umgang mit digitalen Konferenzsystemen:

- Familienmitglieder, Mitbewohner und andere Haushaltsangehörige sowie sonstige Dritte dürfen nicht bei dienstlichen Telefonaten oder Audio-/Videokonferenzen mithören.
- Es ist sicherzustellen, dass bei der Nutzung von Konferenzsystemen eine Einsichtnahme der Informationen durch Dritte (z.B. durch über die Schulter schauen) nicht möglich ist.
- Sprachassistenten von privaten Smart Home Geräten, wie z.B. Amazon Echo Show, sind während Video- oder Audiokonferenzen sowie bei Telefonaten zu deaktivieren (Taste „mute“).
- Die Übergabe der MS Teams Bildschirmsteuerung an Dritte ist untersagt. Ausschließlich das Teilen des Bildschirms ist erlaubt.
- Es dürfen keine Dokumente oder Daten über Microsoft Teams gespeichert, getauscht, transferiert oder empfangen werden, welche eine Klassifikation „vertraulich“ oder „persönlich“ oder höher haben.
- Nutzen Sie, nach Möglichkeit, Dienstgeräte oder von der LWW gestellte Geräte für Audio- und Videokonferenzen.
- Die Nutzung privater Zugangsdaten für dienstliche Audio- oder Videokonferenzen mit der LWW ist untersagt.

Anhang 3: Anhang 3 „Erkennung und Meldung Sicherheitsereignissen und -vorfällen“:

Die Informationssicherheit ist ein Kernanliegen der Leipziger Wasserwerke. Der Betrieb der Wasserwerke hängt immer mehr von Informationen und informationsverarbeitenden Systemen ab. Bewusst oder unbewusst können große Schäden herbeigeführt werden, sofern die etablierten Regelungen nicht eingehalten werden.

Aus diesem Grund möchten wir Ihnen eine Übersicht von verschiedenen Indikatoren an die Hand geben, die es Ihnen erleichtert, potenziell sicherheitsrelevante Ereignisse zu erkennen und entsprechend zu agieren. Bitte melden Sie Sicherheitsereignisse und/ oder -vorfälle unverzüglich an die nachfolgende Kontaktadresse.

Die richtigen Ansprechpartner:

Sie haben einen Sicherheitsvorfall im eigenen Unternehmen oder bei den Leipziger Wasserwerken bemerkt?
Dann wenden Sie sich **unverzüglich** an den LWW IT-ServiceDesk: **Telefon: 0341 969-3666**
E-Mail: it.wasserwerke@L.de

Meldung von Sicherheitsvorfällen mit folgenden Informationen:

- Wann und wo ist der Sicherheitsvorfall eingetreten?
- Welches IT/OT-System oder welcher Standort ist betroffen?
- Was haben Sie am IT/OT-System/am Standort beobachtet?
- Wie haben sie mit dem IT/ OT-System gearbeitet?
- Wie ist es passiert?

Bitte hinterlassen Sie Ihre Kontaktdaten, damit wir Sie für Rückfragen erreichen können.

Indikatoren für Ereignisse mit Potential zum Sicherheitsvorfall

Indikatoren für Social Engineering	Verhalten
• Aufforderung auf Link zu klicken (ggf. sind Buchstaben im Link ausgetauscht) • Absenderadresse entspricht nicht der bekannten Firmenadresse • Nicht erwarteter E-Mail-Anhang • Unpersönliche Anrede bzw. schlechte Rechtschreibung • Vortäuschung von akutem Handlungsbedarf oder Drohungen • E-Mail-Adresse enthält kyrillische Buchstaben, die andere Buchstaben ersetzen (z. B. deutsches „p“ und kyrillisches „r“) oder wird nicht korrekt dargestellt • Verlinkte Seite hat kein TLS-Zertifikat (kein https://) → das „s“ bei https ist wichtig!	1. Der 3-Sekunden Sicherheitscheck für E-Mails (Plausibilitätscheck): – Ist die Absende-Mailadresse bekannt? – Ist der Betreff sinnvoll? – Wird zu diesem Zeitpunkt ein Anhang von dieser E-Mail-Adresse erwartet? 2. Nicht auf verdächtige Links in E-Mails klicken und keine Anhänge öffnen, die nicht erwartet werden. 3. Keine unbekannten Makros ausführen. 4. Stets die URL überprüfen, bevor sie aufgerufen wird (korrekte Adresse, Anhänge, Buchstabendreher etc.?) 5. Bei Unklarheit beim Absender anfragen, beispielsweise telefonisch. **Tipp: Mouseover-Effekt** Sie erkennen die tatsächliche E-Mail-Adresse, indem Sie mit dem Mauszeiger über die E-Mail-Adresse gehen. Dabei wird die tatsächliche/reale E-Mail-Absender-Adresse sichtbar.

Indikatoren für physische Vorfälle	Verhalten
• Offensichtliche Beschädigungen z. B. Schlösser, Telefone, Sicherheitstechnik • Diebstahl [auch vermuteter] • Nicht gekennzeichneter USB-Stick/externer Datenträger liegt herum	1. (Falls möglich) klären, ob die Ursache der Beobachtung sich als harmlos erweist 2. Offensichtliche Beschädigungen bei IT-ServiceDesk melden 3. (Vermuteten) Diebstahl bei IT-ServiceDesk melden 4. Herumliegende USB-Sticks nicht einstecken, sondern direkt bei IT-ServiceDesk melden

Indikatoren für IT-Situationen	Verhalten
• Plötzlicher Absturz oder lange Reaktionszeiten des Systems • Mail-Account ist voll oder reagiert langsam • Datenvolumen des Smartphones ist schneller als gewohnt ausgereizt • Auf dem Rechner tauchen Anwendungen auf, die bis vor Kurzem nicht da waren • Vermehrtes Erscheinen von Werbung • Erscheinen von Sicherheitshinweisen, Zahlungsaufforderungen oder Fenster mit Aufforderung zur Eingabe weiterführender Rechte oder administrativer Accounts • Dateien bzw. Ordner sind unerklärlicherweise gelöscht oder nicht mehr einsehbar	1. Das System nicht weiter benutzen und die weitere Arbeit am IT-System einstellen 2. Das System herunterfahren und Netzwerkkabel trennen 3. Bitte unverzüglich beim IT-Servicedesk der LWW nachfragen bzw. melden und weitere Anweisungen entgegennehmen.