

Geheimhaltungskonzept (Anlage zur Vertraulichkeitsvereinbarung)

Zweck und Geltungsbereich

Dieses Geheimhaltungskonzept definiert verbindliche Maßnahmen zum Schutz vertraulicher Informationen im Rahmen des Wartungs- und Instandhaltungsvertrags für kritische IT-Systeme der Tunnelleitzentrale Berlin. In dieser zentralen Leitstelle werden 12 Tunnelanlagen kontinuierlich überwacht und gesteuert, was sie als kritische Infrastruktur gemäß BSI-Kritisverordnung (BSI-KritisV) und BSIG einstuft. Das Konzept dient als revisionssicherer Anhang zur Vertraulichkeitsvereinbarung zwischen der Autobahn GmbH des Bundes (Niederlassung Nordost) – im Folgenden AG (Auftraggeber) – und dem beauftragten AN (Auftragnehmer). Es regelt umfassend den vertraulichen Umgang mit allen im Vertragsverlauf ausgetauschten Informationen und Unterlagen. Ziel ist ein auditfähiges, juristisch nachweisbares Regelwerk nach aktuellem Stand der Technik, das sicherstellt, dass sämtliche Geschäfts- und Betriebsgeheimnisse wirksam geschützt sind.

Reichweite: Dieses Geheimhaltungskonzept gilt für *alle* Informationen, Dokumente, Daten und Zugänge, die der AN im Zuge der Leistungserbringung vom AG erhält oder verarbeitet, ebenso wie für vom AN generierte Berichte, Protokolle oder sonstige Dokumentationen, die sicherheitsrelevante Details der Anlagen enthalten. Es umfasst technische Betriebsdaten, IT-Konfigurationen, Zugriffsdaten sowie jegliche Informationen über die Struktur, Funktionsweise und Sicherheitsmechanismen der Tunnelanlagen. Auch bei Subunternehmern oder sonstigen Dritten, die ggf. im Auftrag des AN tätig sind, ist die Einhaltung dieses Konzepts sicherzustellen. Ausgenommen sind lediglich Informationen, die nachweislich allgemein öffentlich bekannt oder dem AN bereits vor Vertragsbeginn bekannt waren.

Rechtsgrundlagen und einschlägige Standards

Dieses Konzept orientiert sich an den Anforderungen des deutschen Geschäftsgeheimnisgesetzes (GeschGehG) sowie den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) für kritische Infrastrukturen. Gemäß § 2 Nr. 1 GeschGehG gelten Informationen nur dann als *Geschäftsgeheimnis*, wenn ihr Inhaber angemessene Geheimhaltungsmaßnahmen getroffen hat. Dementsprechend werden in diesem Dokument klare Klassifizierungen, Kennzeichnungen und Schutzmaßnahmen definiert, um den angemessenen Schutzgrad sicherzustellen. Frei nach dem Motto: *Wenn etwas vertraulich ist, muss auch „Vertraulich“ draufstehen* – andernfalls kann keine rechtliche Geheimhaltungswirkung beansprucht werden.

Als Betreiber einer KRITIS-Anlage unterliegt der AG den Pflichten aus dem BSI-Gesetz (BSIG). Insbesondere verlangt § 8a BSIG die Umsetzung *aktueller Stand-der-Technik*-Sicherheitsmaßnahmen. Dieses Konzept trägt dem Rechnung, indem es sich an etablierten Normen orientiert: dem BSI IT-Grundschutz-Kompodium, ISO/IEC 27001 sowie dem branchenspezifischen Sicherheitsstandard (B3S) „Bundesautobahn“ für Verkehrssteuerungs- und Leitsysteme. Letzterer konkretisiert die allgemeinen KRITIS-Anforderungen für den Autobahnsektor und definiert – in Abstimmung mit dem BSI – angemessene Schutzmaßnahmen für Anlagen wie die Tunnelleitzentrale. Durch die Einhaltung dieses Konzepts wird sichergestellt, dass die Vertraulichkeitsvorgaben sowohl gesetzeskonform als auch technisch state-of-the-art sind.

Die Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen der Tunnel-Infrastruktur sind besonders zu schützen. Alle hier beschriebenen Maßnahmen folgen dem

Need-to-know-Prinzip des BSI: Nur Personen, die eine Information zur Erfüllung ihrer Aufgaben zwingend benötigen, erhalten Zugriff. Dadurch wird die Angriffsfläche minimiert und die Anforderungen des BSI-Grundschatzes hinsichtlich Zugriffskontrolle voll erfüllt. Ergänzend findet das Prinzip der Datenminimierung Anwendung: Es werden nur solche Daten ausgetauscht oder gespeichert, die für den Wartungszweck unverzichtbar sind.

Klassifizierung von Informationen und Schutzklassen

Um dem unterschiedlichen Schutzbedarf gerecht zu werden, werden vertrauliche Informationen in vier Schutzklassen eingeteilt. Jede Schutzklasse definiert ein Niveau der Vertraulichkeit und bestimmt konkrete technische und organisatorische Maßnahmen für Umgang und Schutz. Die Einteilung lehnt sich an gängige Informationsklassifizierungsschemata in Wirtschaft und Verwaltung an, wurde jedoch an die besonderen Erfordernisse der Tunnelanlagen (KRITIS) angepasst. Die vier Stufen lauten: „Intern“, „Vertraulich“, „Streng Vertraulich“ und „Kritische Sicherheitsinformation“.

Für jede Schutzklasse werden im Folgenden die Definition, typische Beispiele aus dem technischen Kontext (Netzpläne, Logfiles, Konfigurationen etc.) sowie die verbindlichen Schutzmaßnahmen (für Speicherung, Zugriff, Weitergabe, Löschung und Dokumentation) beschrieben. Grundsätzlich gilt für alle Klassen, dass Informationen stets klar gekennzeichnet werden müssen (siehe Abschnitt Kennzeichnungspflicht weiter unten) und dass bei Aggregationen von Informationen die höchste enthaltene Schutzklasse maßgeblich ist. (Beispiel: Ein Bericht, der mehrere lediglich interne Einzelinformationen zusammenführt, kann insgesamt vertraulich werden und muss dann als „Vertraulich“ behandelt werden.)

Schutzklasse „Intern“

Definition: *Interne Informationen* sind Daten und Unterlagen, die zwar nicht öffentlich bekannt sein sollen, deren unautorisierte Offenlegung jedoch nur geringfügigen Schaden oder Nachteil für die Sicherheit und den Betrieb der Tunnelanlagen bedeuten würde. Diese Klasse umfasst die *Basis-Vertraulichkeitsebene* für den rein internen Gebrauch innerhalb der Autobahn GmbH und des Auftragnehmers.

Beispiele: Routine-Dokumente ohne sicherheitskritische Details oder personenbezogene Daten. Dazu zählen etwa allgemeine Betriebsablaufbeschreibungen, einfache Wartungsberichte ohne sensitive technische Parameter, organisatorische Terminpläne oder Kontaktlisten der beteiligten Personen. Auch Übersichtsunterlagen über die Anlagen, die keine konkreten technischen Spezifikationen (z. B. keine exakten IP-Adressen oder Passwörter) enthalten, können als „Intern“ eingestuft werden. Logfiles mit rein betrieblichen Ereignissen (ohne sicherheitsrelevante Einträge) und ungefähre Datenmengen-Angaben zur Systemnutzung können ebenfalls intern sein, sofern sie keine kritischen Schlüsse erlauben.

Schutzmaßnahmen (Intern):

- Speicherung: *Interne Informationen* dürfen auf den IT-Systemen der Vertragsparteien ohne besondere Zusatzmaßnahmen gespeichert werden, jedoch ausschließlich in internen Bereichen der Organisation. Eine Ablage auf allgemein zugänglichen (öffentlichen) Servern oder Cloud-Diensten ist unzulässig. Zugriffe von außen sind durch Firewall oder VPN zu beschränken.
- Zugriffskontrolle: Der Zugriff ist auf Mitarbeiter des AG und AN begrenzt, die in das Projekt eingebunden sind. Eine Freigabe an Dritte darf nur nach *Need-to-know-Prinzip* erfolgen.

Allgemeiner interner Zugang (z. B. für alle Unternehmensmitarbeiter) sollte vermieden werden, um den Kreis der Wissenden eng zu halten.

- Weitergabe: Interne Informationen können innerhalb der Organisation frei weitergegeben werden, *nicht jedoch nach außen*. An den AN übermittelte interne Unterlagen dürfen dessenseits nur an eigene Mitarbeiter weitergegeben werden, die an diesem Auftrag arbeiten. Externe Weitergabe (an Unterauftragnehmer etc.) bedarf mindestens der Zustimmung des AG. Eine Verschlüsselung bei elektronischer Übermittlung ist für „Intern“ noch nicht zwingend vorgeschrieben, wird aber empfohlen (bspw. Transportverschlüsselung per TLS). Physische Dokumente können betriebsintern verteilt werden, sollten aber nicht offen ausliegen.
- Löschung: Für internes Material gelten reguläre Lösch- und Archivierungsfristen. Ist eine Vernichtung erforderlich, reicht das allgemeine Schutzniveau nach DIN 66399 Sicherheitsstufe 1 (bspw. Aktenvernichter Partikelschnitt für Papier). Digitale Daten werden mindestens durch einfaches Überschreiben gelöscht.
- Dokumentation: Ein gesondertes Protokoll über die Nutzung interner Informationen ist nicht vorgeschrieben. Allerdings sollen Herausgabe und Rückgabe interner Unterlagen zum Vertragsende dokumentiert werden, um vollständige Rückführung zu gewährleisten. Nicht gekennzeichnete Dokumente werden standardmäßig als „Intern“ behandelt.

Schutzklasse „Vertraulich“

Definition: *Vertrauliche Informationen* sind Daten, deren unbefugte Veröffentlichung den sicheren Betrieb der Tunnelanlagen oder die Interessen des AG spürbar beeinträchtigen könnte. Sie sind nur einem begrenzten Personenkreis zugänglich und unterliegen erhöhten Schutzanforderungen, aber noch nicht der höchsten Sicherheitsstufe. Diese Klasse entspricht in etwa dem üblichen Unternehmensgeheimnis oder sensiblen Betriebsgeheimnis, das durch NDA/Geheimhaltungsvereinbarung abgedeckt wird.

Beispiele: Technische Unterlagen und digitale Daten mit detaillierteren, jedoch nicht sicherheitskritischsten Inhalten. Hierunter fallen z. B. Teil-Netzwerkpläne oder Topologieskizzen der Tunnel-IT (ohne vollständige Netzabdeckung), Übersichten der verwendeten IP-Adressbereiche und VLAN-Zuordnungen in weniger kritischen Segmenten, sowie Konfigurationsdaten von Standardsoftware (etwa Server-Betriebssystem-Einstellungen), sofern sie keine direkten Zugänge erlauben. Typische Logfiles aus den Steuerungssystemen, die allgemeine Betriebszustände protokollieren (und keine sicherheitsrelevanten Vorfälle oder personenbezogenen Daten enthalten), sind vertraulich. Ebenso könnten Aufstellungen über Datenmengen, Speicherplatzbelegung oder technische Inventarlisten (Hardware- und Softwarestände der Anlage) in diese Kategorie fallen. Insgesamt gilt: Informationen, die einem Angreifer bereits nützen könnten, aber für sich genommen noch keine unmittelbare Kompromittierung ermöglichen, sind „Vertraulich“.

Schutzmaßnahmen (Vertraulich):

- Speicherung: Vertrauliche Informationen sind in zugriffsgeschützten Bereichen der IT-Systeme aufzubewahren. Das bedeutet, sie dürfen nur auf Servern/Laufwerken liegen, die durch Berechtigungskonzepte vor unbefugtem Zugriff geschützt sind (z. B. Projektlaufwerke mit Zugangsbeschränkung). Cloud-Speicherung ist nur zulässig, wenn der Cloud-Dienst innerhalb der EU betrieben wird und vertraglich dem Datenschutz und der Vertraulichkeit verpflichtet ist. In jedem Fall müssen vertrauliche Daten auf mobilen Datenträgern oder Laptops verschlüsselt gespeichert werden (z. B. durch Festplattenverschlüsselung), um Schutz bei Verlust sicherzustellen.

- Zugriffskontrolle: Der Zugriff auf „Vertraulich“ eingestufte Informationen ist auf einen eng definierten Personenkreis zu beschränken. Dies umfasst typischerweise die unmittelbaren Projektmitarbeiter und ggf. ausgewählte Vertreter des AG. Zugriff wird über personalisierte Nutzerkonten geregelt; gemeinsame Team-Logins sind zu vermeiden. Role-Based Access Control (RBAC) soll sicherstellen, dass nur Personen mit entsprechender Rolle (Wartungsingenieur, Projektleiter etc.) die Daten einsehen können. Alle berechtigten Personen sind ausdrücklich zur Geheimhaltung zu verpflichten (schriftliche Verpflichtungserklärung).
- Weitergabe: Eine Weitergabe vertraulicher Informationen *innerhalb* der Organisation des AG oder AN erfolgt nur, wenn erforderlich, vorzugsweise end-to-end verschlüsselt (etwa per E-Mail mit TLS und zusätzlich Dateiverschlüsselung). Extern dürfen solche Informationen nur an ausdrücklich autorisierte Dritte gegeben werden – etwa Unterauftragnehmer – und auch dann ausschließlich gegen Unterzeichnung einer eigenen Vertraulichkeitsvereinbarung (NDA). Beim Versand physischer Dokumente ist ein versiegelter Umschlag zu verwenden, der als „Vertraulich“ gekennzeichnet ist. Jede externe Herausgabe ist vom AN vorab vom AG genehmigen zu lassen.
- Löschung: Vertrauliche Dokumente sind, sobald sie nicht mehr benötigt werden, sicher zu löschen oder zu vernichten. Papierunterlagen sind mindestens nach DIN 66399 Sicherheitsklasse 2 zu schreddern (feine Partikelzerteilung). Elektronische Daten sind durch Überschreiben mit geeigneten Tools oder durch Kryptografisches Löschen (Crypto-Shredding) zu entfernen. Der AN richtet interne Prozesse ein, um regelmäßig zu prüfen, ob vertrauliche Daten noch benötigt werden, und sie sonst zu löschen.
- Dokumentation: Der AN führt ein Verzeichnis aller vom AG erhaltenen vertraulichen Dokumente/Daten. Jede Weitergabe an Dritte oder Kopie wird darin vermerkt. Zugriffe auf zentrale Ablagen sollen protokolliert werden (etwa mittels Windows Event Logging oder DMS-Protokollen), sodass nachvollziehbar bleibt, wer wann welche vertrauliche Information abgerufen hat. Diese Protokolle dienen der Nachvollziehbarkeit für Audits. Zudem empfiehlt es sich, quartalsweise interne Überprüfungen der Klassifizierungen durchzuführen, um sicherzustellen, dass keine Anpassungen nötig sind (z. B. ob Dokumente herauf- oder herabzustufen sind).

Schutzklasse „Streng Vertraulich“

Definition: *Streng vertrauliche Informationen* sind äußerst sensible Daten, deren Kompromittierung schwerwiegende Konsequenzen für die Betriebssicherheit, Verfügbarkeit der Tunnel oder die öffentliche Sicherheit haben könnte. Diese Kategorie entspricht dem höchsten Schutzbedarf unter „normalen“ Betriebsgeheimnissen und wird nur an engste, benannte Personengruppen freigegeben. Informationen dieser Stufe sind in der Regel nur wenigen Führungskräften, Sicherheitsverantwortlichen oder speziell autorisierten Technikern bekannt. Eine Verletzung der Vertraulichkeit würde erhebliche Risiken, Schäden oder Rechtsverstöße nach sich ziehen.

Beispiele: Vollständige Netzwerkpläne der Tunnelleitzentrale und aller angebundenen Tunnelanlagen mit detaillierter Darstellung sämtlicher Komponenten, Verbindungen und Sicherungseinrichtungen. Topology-Diagramme, die die genaue Kopplung von IT- und OT-Systemen (Steuerrechner, Sensorik, Aktorik) abbilden. Softwarekonfigurationen sicherheitsrelevanter Systeme – etwa die exakten Einstellungen der Tunnelsteuerungssoftware, SCADA-Systeme oder Firewalls. Ausführliche Logfiles oder Protokolldateien, die sicherheitskritische Ereignisse dokumentieren (z. B. Fehlermeldungen von Sicherheitsfunktionen, ungewöhnliche Zugriffsmuster) oder personenbezogene bzw. betreiberkritische Daten enthalten. Angaben zu Schnittstellen und Systemabhängigkeiten, die aufzeigen, wie verschiedene Teilsysteme (Beleuchtung, Belüftung, Notruf, Leitsystem etc.) interagieren und welche Rückfallebenen existieren. Auch Übersichten über Benutzerkonten und

Zugriffsrechte in den Systemen – ohne jedoch konkrete Passwörter zu nennen – zählen hierher, da sie einem Angreifer wertvolle Anhaltspunkte für mögliche Angriffspfade liefern würden. Streng vertraulich sind ferner interne Notfallpläne oder Schwachstellenanalysen der Anlage. Insgesamt gilt: Informationen, die ein umfassendes technisches Lagebild der Infrastruktur vermitteln oder Schlüsseldetails zu ihrer Sicherung enthalten, sind „Streng Vertraulich“.

Schutzmaßnahmen (Streng Vertraulich):

- **Speicherung:** Streng vertrauliche Daten dürfen ausschließlich in hochsicheren IT-Umgebungen gespeichert werden. Dies umfasst z. B. speziell abgesicherte Server des AG (oder AN) mit eingeschränktem Personenkreis, getrennt vom normalen Büronetz. Eine Ablage muss stets verschlüsselt erfolgen (z. B. Datei- oder Volumenverschlüsselung mit starken Algorithmen). Cloud-Speicherung ist untersagt, es sei denn, der AG erteilt eine ausdrückliche Ausnahmegenehmigung und die Cloud erfüllt höchste Sicherheitsstandards. Mobile Datenträger (USB-Sticks, Laptops) sind für streng vertrauliche Daten nur zulässig, wenn sie vom AG vorher genehmigt und hardwareverschlüsselt sind. Eine physische Trennung dieser Daten von weniger sensiblen ist anzustreben (z. B. separate Netzwerksegmente oder Container).
- **Zugriffskontrolle:** Der Zugang ist nur einzelnen namentlich benannten Personen gestattet. In der Regel sind dies Projektleiter auf Seiten AG/AN, der Informationssicherheitsbeauftragte (CISO) und ggf. ausgewählte Administratoren, die solche Daten zur Aufgabenerfüllung benötigen. Zugriffe sollten durch starke Authentisierungsmechanismen geschützt werden – mindestens 2-Faktor-Authentisierung (z. B. Smartcard oder One-Time-Token) für die Benutzerkonten. Alle Berechtigungen für diese Klasse sind regelmäßig (mindestens alle 6 Monate) zu überprüfen und bei Personenwechseln sofort zu widerrufen. Die Nutzung von Gruppen-Accounts ist absolut verboten; individuelle Accountability muss gewährleistet sein. Zudem ist der Zugriff, wenn möglich read-only zu gestalten, um Manipulationen vorzubeugen (sofern nicht zur Aufgabenerfüllung Schreibrechte nötig sind).
- **Weitergabe:** Eine Weitergabe streng vertraulicher Informationen erfolgt nur in absoluten Ausnahmefällen. Der Standardfall ist: keine externe Weitergabe. Sollte der AN solche Informationen vom AG erhalten, dürfen sie *nicht* an Unterauftragnehmer oder sonstige Dritte weitergegeben werden, es sei denn der AG stimmt schriftlich zu und die Drittpartei unterzeichnet ebenfalls eine vergleichbare Geheimhaltungsverpflichtung. Intern beim AN dürfen diese Informationen nicht per normaler E-Mail verschickt werden; stattdessen ist ein vom AG freigegebenes sicheres Kommunikationsverfahren zu nutzen (z. B. verschlüsselte Dateiübertragung via SFTP oder ein vom AG bereitgestelltes geschütztes Portal). Bei unvermeidbarer physischer Weitergabe (z. B. Datenträger) sind diese persönlich zu übergeben oder per Kurier in doppeltem Umschlag, *innen* gekennzeichnet als „Streng Vertraulich“ und *außen* neutral. Jeder Transfer ist vorab vom Informationssicherheitsbeauftragten zu autorisieren und im Übergabeprotokoll festzuhalten.
- **Löschung:** Streng vertrauliches Material ist nach Verwendung unverzüglich aus den Systemen des AN zu entfernen, sofern keine weitere Aufbewahrungspflicht besteht. Digitale Daten sind mittels kryptografischer Löschung oder physischer Vernichtung der Datenträger zu beseitigen. Beispielsweise kann bei verschlüsselten Datenspeichern der Schlüssel gelöscht (Crypto-Shredding) und das Medium überschrieben werden. Papierdokumente sind durch einen Aktenvernichter der Sicherheitsstufe 3 gemäß DIN 66399 zu vernichten (Partikelgröße < 320 mm²). Die Löschung/Vernichtung ist zu protokollieren und vom Sicherheitsverantwortlichen zu prüfen. Zum Vertragsende muss der AN dem AG schriftlich bestätigen, dass sich keine streng vertraulichen Informationen des AG mehr in seinem Besitz befinden (oder diese an den AG zurückgegeben bzw. zerstört wurden).

- **Dokumentation:** Für alle streng vertraulichen Informationen wird ein streng geführtes Zugriffsprotokoll verlangt. Jeder Zugriff (Öffnen, Kopieren, Bearbeiten) auf entsprechende Dateien oder Ordner soll automatisiert protokolliert werden (Benutzer, Zeitpunkt, Art des Zugriffs). Diese Protokolle sind mindestens jährlich auszuwerten, um unautorisierte Zugriffe auszuschließen. Weiterhin ist ein Verzeichnis der Dokumente zu führen, aus dem hervorgeht, wer die Originale oder Kopien besitzt. Etwaige Audit-Trails müssen gemäß Vorgaben des BSI so aufbewahrt werden, dass sie manipulationssicher und für Prüfungen verfügbar sind. Der AG behält sich vor, jederzeit eine Einsicht in diese Nachweise zu verlangen. Im Rahmen der KRITIS-Compliance sind so umfangreiche Dokumentationspflichten zu erfüllen, dass alle sicherheitsrelevanten Maßnahmen und Prozesse nachvollziehbar aufgezeichnet sind. Diese Dokumentation dient als Nachweis gegenüber Auditoren (BSI, interne Revision) und muss daher vollständig und aktuell gehalten werden.

Schutzklasse „Kritische Sicherheitsinformation“

Definition: *Kritische Sicherheitsinformationen* stellen die höchste Vertraulichkeitsstufe in diesem Konzept dar. Darunter fallen Informationen, die direkt die betriebskritischsten Sicherheitsfunktionen der Tunnelanlagen betreffen und bei Bekanntwerden unmittelbar eine Gefährdung der Anlage, der öffentlichen Sicherheit oder der Integrität des Gesamtsystems nach sich ziehen würden. Diese Kategorie geht über „streng vertraulich“ hinaus, indem sie solche Details umfasst, deren Schutz für die Aufrechterhaltung der Sicherheit *essenziell* ist. Diese Informationen sind mit behördlichen Verschlussachen vergleichbar und unterliegen maximalen Schutzvorkehrungen. Zugriff darauf erhalten nur ausgewählte Personen mit besonderer Autorisierung, ggf. nach zusätzlicher Sicherheitsüberprüfung.

Beispiele: *Authentisierungs- und Zugangsdetails* zu den Systemen der Tunnelanlage. Hierzu zählen insbesondere Zugangsdaten, Passwörter oder kryptographische Schlüssel für Administratoren der Tunnelleitzentrale oder der angeschlossenen Steuer- und Betriebssysteme. Insbesondere alle Informationen zu Remote-Zugriffen sind in dieser Klasse eingeordnet: Konfigurationen und Zugangsdetails von VPN-Verbindungen, Einstellungen des Cisco DUO Multifaktor-Authentifizierungssystems (z. B. Enrollment-Daten, Token-Generierungsverfahren), sowie die technischen Verfahren zur Fernwartung (etwa spezielle IPs/Ports für Fernzugriff, Notfall-Fernwartungssaccounts). Des Weiteren zählen Master-Passwörter, SSH-Schlüssel oder Zertifikate zur Absicherung der Tunnel-IT hierher. Genau Kenntnis der Schnittstellen zwischen IT und OT auf tiefster Ebene (z. B. direkte Zugriffsmöglichkeiten vom Leitstand in die Steuerung) und Exploit-Details von Schwachstellen, die in der Anlage entdeckt, aber noch nicht behoben sind, werden ebenfalls als kritischste Sicherheitsinformationen betrachtet. Kurzum: Alles, was einem Angreifer ermöglichen würde, *unmittelbar* Kontrolle über Systeme zu erlangen oder Sicherheitsmechanismen auszuhebeln, fällt in diese höchste Schutzklasse.

Schutzmaßnahmen (Kritische Sicherheitsinformation):

- **Speicherung:** Solche Informationen sollen *nach Möglichkeit überhaupt nicht persistent gespeichert* werden, sondern nur im flüchtigen Zugriff gehalten. Unvermeidbare Speichervorgänge (z. B. Ablage von Passwortlisten, VPN-Schlüsseln) müssen in gesonderten Hochsicherheits-Speichern erfolgen. Beispielsweise können vom AG bereitgestellte Hardware-Sicherheitsmodule oder speziell gesicherte Tresor-Systeme (Password Vaults) genutzt werden. Eine Speicherung auf üblichen IT-Systemen des AN ist untersagt, es sei denn, der Bereich wurde vom AG explizit geprüft und freigegeben. In diesem Fall ist eine starke Verschlüsselung mit vom AG vorgegebenen Schlüsseln zwingend. *Hinweis:* Oft wird der AG vermeiden, derartige Daten überhaupt dem AN auszuhändigen; sollte es dennoch erforderlich sein (etwa temporäre Admin-Passwörter für Wartungszwecke), werden diese nur nach diesem Konzept übergeben und ggf. nach Nutzung sofort geändert.
- **Zugriffskontrolle:** Zugriff erhalten nur die vom AG speziell ermächtigten Personen – in vielen Fällen dürfte das auf einzelne Sicherheitsadministratoren beschränkt sein. Der AN muss dafür sorgen, dass innerhalb seiner Organisation nur konkret benannte Fachkräfte (z. B. ein Security-Engineer) Einblick in diese Informationen erhalten, und auch nur für die minimal nötige Dauer. Jeder Zugriff muss zusätzlich zum normalen Authentifizierungsverfahren mit einem vier-Augen-Prinzip gekoppelt werden, d.h. eine zweite berechnigte Person oder der AG selbst autorisiert den Zugriff jeweils. Technisch ist der Einsatz von MFA (Multi-Factor Authentication) Pflicht, idealerweise kombiniert mit Hardware-Token oder Smartcard, um höchste Sicherheit zu gewährleisten. Systeme, auf denen kritische Sicherheitsinformationen angezeigt oder genutzt werden, dürfen keine Internetverbindung haben und müssen gegen Datenträgerexport gesichert sein. Es wird empfohlen, dedizierte vom AG gestellte Laptops oder Terminalsysteme für solche Zugriffe zu verwenden, um die Umgebung vollständig kontrollieren zu können.
- **Weitergabe:** Eine Weitergabe dieser Informationen ist *nur mit schriftlicher Einzelgenehmigung* des AG zulässig. In der Praxis bedeutet dies, dass z. B. Passwörter oder VPN-Zugangsdaten vom AG direkt an eine benannte Person beim AN übermittelt werden (in der sichersten möglichen Form, z. B. persönlich vor Ort oder via geteilte Geheimnisse in einem Passwort-Manager). Der AN darf solche Daten keinesfalls an Dritte weiterleiten. Falls der AN interne Mitarbeiter wechseln muss, ist die Übergabe intern genauso restriktiv zu handhaben und dem AG anzuzeigen. Elektronische Übertragung solcher Informationen ist möglichst zu vermeiden; falls unumgänglich, muss eine Ende-zu-Ende-Verschlüsselung mit vorher ausgetauschten Schlüsseln genutzt werden (keine Übermittlung per normaler E-Mail oder Chat). Einmal genutzt, sollen z. B. temporäre Passwörter sofort durch neue vom AG ersetzt werden, sodass ein evtl. abgeflossenes altes Passwort wertlos wäre.
- **Löschung:** Kritische Sicherheitsdaten sind *sofort nach Gebrauch* sicher zu vernichten. Wurden sie nur im RAM eines Systems gehalten, ist das System anschließend kontrolliert herunterzufahren (um das RAM zu löschen). Wurden sie schriftlich notiert (z. B. auf Papier beim Eintippen eines Passworts), ist dieses Papier unverzüglich zu schreddern (mindestens Sicherheitsstufe 3, besser Verbrennen in Sicherheitsprotokoll). Digitale Dateien (etwa kryptographische Schlüssel) sind nach Nutzung überschrieben und der Schlüssel zu zerstören. Der Vorgang ist durch eine zweite Person zu kontrollieren und im Sicherheitsprotokoll zu vermerken. Sollte der AG verlangen, dass bestimmte Schlüssel oder Zugangsdaten nach Vertragserfüllung zurückgegeben werden, erfolgt dies persönlich oder in Absprache durch

einen hochgesicherten Kanal. Andernfalls bestätigt der AN schriftlich die vollständige Löschung.

- Dokumentation: Jedweder Umgang mit kritischen Sicherheitsinformationen ist *vollständig zu protokollieren*. Dies umfasst: wann und von wem die Information erhalten wurde; wo sie gespeichert wurde; wer darauf zugegriffen hat (mit Zeitpunkt und Zweck); wann sie gelöscht wurde. Dieses Protokoll wird vom AN geführt, vom Informationssicherheitsbeauftragten des AG gegengezeichnet und bei Bedarf dem BSI-Auditor vorgelegt. Aufgrund der hohen Sensibilität ist auch zu dokumentieren, welche Schutzmaßnahmen konkret ergriffen wurden (z. B. „Passwort XY am Datum Z in Tresor ABC gelegt, Zugriff nur durch Person P, gelöscht am Datum Q via Verfahren XY“). Damit wird die Auditierung dieser Maßnahmen ermöglicht. Der AG behält sich vor, unangekündigt Prüfungen durchzuführen, ob beim AN alle Vorgaben für diese Schutzklasse eingehalten werden – z. B. in Form von Sicherheitsaudits oder Penetrationstests auf die entsprechenden Systeme. Die Einhaltung dieser höchsten Geheimhaltungsstufe ist für den Vertrag essenziell; jeder Verstoß würde als *wesentlicher Vertragsbruch* gewertet.

Besondere Behandlung von Remote-Zugriffen und Fernwartung

Remote-Zugriffe (Fernzugriffe) stellen einen Sonderfall dar, der in diesem Konzept differenziert und mit höchster Sorgfalt behandelt wird. Gemäß den BSI-Empfehlungen sind Fernwartungszugänge eines der kritischsten Elemente in Industrienetzen, da sie potenziell mehrere Einfallstore für Angreifer öffnen. Für die Tunnelleitzentrale Berlin kommen Remote-Zugriffe etwa in Form von VPN-Verbindungen vom AN in das Anlagen-Netz oder Home-Office-Zugriffen von berechtigten Personen zum Einsatz. Diese Zugriffe werden als „Kritische Sicherheitsinformation“ im Sinne der obigen Klassifizierung betrachtet, da ihre Sicherung absolut entscheidend ist, um unbefugte Eingriffe in die Tunnelsteuerung zu verhindern.

Klassifizierung: Alle technischen und organisatorischen Details, die mit dem Fernzugriff zusammenhängen – VPN-Configs, IP-Adressen der Zugangspunkte, Zugangsdaten, MFA-Verfahren (z. B. Cisco DUO), verwendete Token oder Zertifikate – sind mindestens als Streng Vertraulich, überwiegend jedoch als Kritische Sicherheitsinformation eingestuft. Insbesondere Zugangsdaten für die VPN/Fernwartung werden in die höchste Schutzklasse eingeordnet.

Zugriffsverfahren: Der Vertrag gestattet einen Fernzugriff des AN *nur in ausdrücklich genehmigter Weise*. Konkret bedeutet dies: Der AG schaltet bei Bedarf einen Wartungszugang (VPN-Tunnel) frei, der AN authentisiert sich zwei-faktor mittels persönlichen Zertifikats und DUO-Token. Jeder Verbindungsaufbau erfolgt von innen nach außen initiiert (d.h. die Anlage baut die Verbindung zum AN auf, nicht umgekehrt), sofern möglich, und muss durch einen internen Verantwortlichen beim AG manuell freigegeben werden. Diese Architektur (zentrale Freigabe, DMZ-gekoppelte Fernwartungskomponente) reduziert das Risiko unautorisierter Zugriffe.

Besondere Schutzmaßnahmen: Remote-Verbindungen sind stets verschlüsselt mit aktuellen, als sicher geltenden Protokollen (z. B. IPsec oder TLS 1.3). Ein starkes Authentisierungsverfahren (Nutzerkonto + Passwort + DUO-Push oder Hardware-Token) ist vorgeschrieben. Die Zugriffsrechte via Fernwartung sind maximal granular zu gestalten: Der AN erhält nur Zugang zu den *Systemen, die für die jeweilige Wartungsaufgabe nötig sind*, und auch dort nur mit eingeschränkten Rechten (Prinzip der minimalen Rechte). Der Fernwartungs-Account des AN wird nach jeder Nutzung sofort wieder deaktiviert oder zeitlich begrenzt eingerichtet. Automatische Sitzungstrennung: Jede Fernwartungssitzung ist vom AG nach Auftragsende zu beenden; es darf kein Dauer-VPN aktiv bleiben.

Protokollierung und Kontrolle: Jeder Remote-Zugriff wird lückenlos protokolliert. Beginn und Ende der Sitzung, zugriffene Systeme, durchgeführte Aktionen werden erfasst. Der AN hat bei jeder Fernwartungsaktion außerdem eine Meldepflicht an die Leitstelle (z. B. telefonische Anmeldung beim Start und Ende, gemäß vertraglicher Vorgabe), um sicherzustellen, dass das Betriebspersonal vor Ort den Remote-Zugriff überwacht. Unregelmäßigkeiten oder Auffälligkeiten während der Fernwartung (z. B. Verbindungsabbrüche, Fehlermeldungen) sind sofort zu melden. Zusätzlich empfiehlt das BSI den Einsatz von Intrusion-Detection-Systemen an den Fernwartungszugängen, um unautorisierte Versuche abzuwehren – der AG hat hierfür entsprechende Systeme implementiert.

Heimarbeitsplätze: Sofern Mitarbeiter des AN von einem Heimarbeitsplatz auf die Tunnel-Systeme zugreifen, gelten strenge Auflagen: Der genutzte Rechner muss den Sicherheitsanforderungen des AG genügen (aktuelles Antivirenprogramm, Firewall, keine privaten Nutzungen während der Sitzung, abgeschirmter Arbeitsplatz). Der Tunnelzugang vom Home-Office ist technisch dem vom Firmennetz gleichgestellt, d.h. ebenfalls VPN + MFA. Es wird seitens AN sichergestellt, dass im Home-Office keine weiteren Personen Zugang zum Bildschirm oder zu Notizen mit Zugangsdaten haben.

Durch diese differenzierte Behandlung der Remote-Zugriffe wird dem Umstand Rechnung getragen, dass gerade hier ein sehr hohes Risiko besteht. Laut BSI werden Fernzugriffsmöglichkeiten oft von Angreifern ausgenutzt, wenn sie unzureichend gesichert sind. Daher gilt: Remote-Zugriff nur sparsam und kontrolliert einsetzen (Minimalitätsprinzip), Zugänge härten und überwachen, Informationen darüber streng geheim halten.

Kennzeichnungspflicht

Alle herausgegebenen Informationen und Dokumente müssen eindeutig gekennzeichnet werden, damit ihr Schutzstatus jederzeit erkennbar ist. Die Kennzeichnung erfolgt gemäß der oben definierten Schutzklassen und stellt sicher, dass Empfänger und Bearbeiter unmittelbar wissen, wie das Dokument zu behandeln ist. Folgende Richtlinien sind anzuwenden:

- Dokumente (Papier): Jedes physische Dokument trägt in der Kopf- oder Fußzeile jeder Seite einen Vermerk der Vertraulichkeitsstufe. Beispiel: „*Vertraulich – Anlage Wartungsvertrag Tunnelbetrieb*“ oder „*Streng Vertraulich – Kritische Sicherheitsinformation*“ in roter Schrift am oberen Rand. Alternativ kann ein Stempel oder Aufdruck auf dem Deckblatt verwendet werden, der die Schutzklasse ausweist. Für besonders kritische Dokumente empfiehlt es sich, farbige Markierungen zu nutzen (z. B. roter Rand für „Streng Vertraulich“).
- Elektronische Dokumente: Die Dateinamen sollen die Klassifizierung enthalten (z. B. „[VERTRAULICH]_Wartungsbericht.pdf“). In digitalen Dokumenten wie Word/PDF ist auf der ersten Seite deutlich anzugeben, in welcher Schutzklasse der Inhalt fällt. Zudem sollen, wenn technisch möglich, Metadaten-Tagging genutzt werden (etwa die Verwendung des eingebetteten Dokumenteneigenschaft-Feldes „Klassifizierung“ in Office-Dokumenten). E-Mails, mit denen vertrauliche Informationen versendet werden, erhalten im Betrefffeld eine eckige Klammer mit dem Klassifizierungswort, z. B. „[INTERN]“, „[VERTRAULICH]“ etc., um dem Empfänger direkt das Schutzniveau anzuzeigen. Zusätzlich ist in der E-Mail selbst vor dem eigentlichen Inhalt ein Hinweistext einzufügen („Dieses Schreiben enthält Informationen der Schutzklasse XY ...“).
- Nicht-textuelle Daten: Für Datenträger (USB-Sticks, Festplatten) oder Geräte, die vertrauliche Informationen enthalten, erfolgt die Kennzeichnung durch Aufkleber oder Anhänger mit der jeweiligen Schutzklasse. Beispiel: Ein USB-Stick mit Konfigurationsdaten wird mit „Streng Vertraulich“ beschriftet. In IT-Systemen können kritische Datenbanken oder Dateien mit entsprechenden Labels in der Rechteverwaltung versehen werden.

- **Fehlende Kennzeichnung:** Sollte ein Dokument ausnahmsweise keine Kennzeichnung tragen, ist *im Zweifel vom höheren Schutzbedarf auszugehen*. Nach Vorgabe des BSI wird meist vereinbart, dass unmarkierte Dokumente automatisch als „Intern“ gelten. Im vorliegenden Vertragsverhältnis verständigen sich AG und AN darauf, dass alle übergebenen Informationen mindestens intern sind – tatsächlich werden die meisten jedoch explizit gekennzeichnet.

Die Kennzeichnungspflicht stellt sicher, dass insbesondere beim AN jede empfangene Unterlage sofort richtig einsortiert und behandelt wird. Sie unterstützt auch dabei, Verstöße zu vermeiden, da Mitarbeiter visuell gewarnt werden, bevor sie etwa ein „Streng Vertraulich“-Dokument kopieren oder versenden. Der AN sorgt durch Schulungen dafür, dass alle Mitwirkenden Personen die Kennzeichnungen verstehen und die daraus resultierenden Handlungsanforderungen kennen.

Protokollierung, Audit-Fähigkeit und Kontrolle

Zur Gewährleistung der Wirksamkeit dieses Geheimhaltungskonzepts werden umfangreiche Protokollierungs- und Kontrollmaßnahmen implementiert. Nur durch eine konsequente Überwachung und Auditierung lässt sich sicherstellen, dass die festgelegten Regeln jederzeit eingehalten werden und im Fall von Sicherheitsvorfällen eine lückenlose Nachvollziehbarkeit gegeben ist. Der Anspruch des AG ist ein *prüffestes* System, das sowohl internen Kontrollen als auch externen Audits (z. B. durch BSI oder andere Aufsichtsbehörden) standhält.

Protokollierung: Für alle vertraulichen, streng vertraulichen und kritischen Informationen müssen geeignete Log-Dateien oder Journal-Einträge geführt werden, die jeden relevanten Zugriff und Vorgang erfassen. Insbesondere die Entnahme oder Einsichtnahme in Streng Vertraulich und kritisch eingestufte Daten ist automatisch zu protokollieren (durch System-Logs) und zusätzlich vom jeweiligen Mitarbeiter in einem manuellen Register zu vermerken. Die Protokolle enthalten Datum/Uhrzeit, beteiligte Person, Art der Aktion (Lesen, Kopieren, Löschen, Übermitteln) und ggf. den Zweck. Sie werden gegen unbefugte Änderung geschützt (Manipulationssicherheit, z. B. durch sichere Syslog-Server oder Blockchain-basierte Audit-Trails). Wichtig ist, dass auch Weitergaben von Dokumenten dokumentiert werden: wer hat wann welche Datei an wen geschickt oder übergeben. Bei physischen Dokumenten kann dies etwa durch Übergabeprotokolle mit Unterschrift erfolgen.

Aufbewahrung der Protokolle: Alle Log- und Protokolldaten zur Geheimhaltung sind für eine angemessene Dauer aufzubewahren, mindestens jedoch für 2 Jahre nach Vertragsende. Dies stellt sicher, dass selbst zeitversetzte Audits (wie die regelmäßigen §8a BSIG-Prüfungen im 2-Jahres-Turnus) auf die relevanten Nachweise zurückgreifen können. Digitale Logs sollten regelmäßig gesichert und archiviert werden (idealerweise in einem *revisionssicheren* Audit-Trail-Archiv).

Audit-Fähigkeit: Der AN verpflichtet sich, dem AG und ggf. Prüfern (z. B. Auditoren im Rahmen des KRITIS-Audits) auf Verlangen Einsicht in die Dokumentation und Protokolle zu geben. Dies umfasst insbesondere: das Verzeichnis klassifizierter Informationen, Nachweise der Kennzeichnung, Zugriffsprotokolle, Löschbestätigungen sowie Schulungsnachweise der Mitarbeiter. Der AG oder von ihm benannte Dritte dürfen Audits durchführen, um die Einhaltung der in diesem Konzept festgelegten Maßnahmen zu überprüfen. Solche Audits können in Form von Vor-Ort-Prüfungen, technischen Überprüfungen (Penetrationstests der relevanten IT des AN) oder Dokumentenprüfungen stattfinden. Der AN hat entsprechende Audits zu ermöglichen und zu unterstützen. Festgestellte Mängel müssen unverzüglich behoben werden; schwerwiegende Verstöße gelten als erheblicher Vertragsverstoß, der Sanktionen nach sich ziehen kann.

Interne Kontrollen: Unabhängig von externen Audits richtet der AN interne Kontrollmechanismen ein. Dazu zählen regelmäßige Self-Assessments bzw. Interne Audits zur Geheimhaltungspraxis, etwa *vierteljährlich* eine Überprüfung durch den Informationssicherheitsbeauftragten des AN, ob alle vertraulichen Dokumente korrekt gekennzeichnet und geschützt sind, ob Zugriffsrechte aktuell sind etc.. Ergebnisse dieser internen Audits sind zu dokumentieren und dem AG auf Wunsch auszuhändigen. Zudem ist ein Eskalationsprozess definiert: Bei Verdacht auf Geheimnisverstoß oder Schwachstellen (z. B. unsachgemäße Lagerung eines vertraulichen Dokuments) informiert der AN umgehend den AG und leitet Gegenmaßnahmen ein.

Schulung und Sensibilisierung: Eine wirksame Kontrolle setzt informierte Mitarbeiter voraus. Der AN stellt sicher, dass alle Personen, die mit klassifizierten Informationen arbeiten, eine angemessene Sensibilisierung erfahren haben. Mindestens jährlich – und zu Projektbeginn – erfolgt eine Schulung über die geltenden Geheimhaltungsregeln, die Schutzklassen und den richtigen Umgang mit entsprechenden Daten. Die Mitarbeiter werden ausdrücklich auf die Folgen von Verstößen hingewiesen und lernen, verdächtige Vorgänge zu melden. Dies schafft ein Klima, in dem Geheimhaltung als Teil der Sicherheitskultur gelebt wird.

Nachweisbarkeit: Schließlich zielt dieses Konzept darauf ab, im Bedarfsfall (z. B. vor Gericht bei Auseinandersetzungen nach GeschGehG) die juristische Nachweisbarkeit des Geheimnisschutzes zu erbringen. Durch die schriftliche Fixierung aller Maßnahmen hier und die Protokollierung ihrer Umsetzung kann der AG jederzeit darlegen, dass seine Geschäftsgeheimnisse durch *angemessene Geheimhaltungsmaßnahmen* geschützt waren. Dieses Dokument selbst wird als Anlage zum Vertrag genommen und beidseitig unterzeichnet, sodass es integraler Vertragsbestandteil ist. Änderungen an diesem Konzept sind nur in Schriftform und im Einvernehmen beider Parteien möglich (§ 21 des Hauptvertrags: Schriftformklausel), um die Revisionssicherheit zu gewährleisten. Jede Version erhält eine Versionsnummer und Datum, um nachvollziehbar zu halten, welche Regelungen wann galten.

Durch die Kombination aus klarer Klassifizierung, technischen und organisatorischen Schutzmaßnahmen, strikter Kennzeichnung, sorgfältiger Protokollierung und regelmäßiger Auditierung erfüllt dieses Geheimhaltungskonzept die Anforderungen des GeschGehG und der BSI-Standards in vollem Umfang. Es gewährleistet einen *stand-der-Technik-Schutz* für alle sensiblen Informationen der Tunnelsteuerungsanlagen und stellt sicher, dass der Betrieb der kritischen Infrastruktur Berlin Tunnel nicht durch Informationsabflüsse gefährdet wird. Beide Vertragsparteien erkennen die bindende Wirkung dieser Vorgaben an und tragen gemeinsam Verantwortung für deren Umsetzung und kontinuierliche Einhaltung.