DAIMLER

Anlage 1 zum Engineering IT-Rahmenvertrag
Ergänzende Anforderungen (Allgemeine Sicherheitsvorkehrungen)

1. Gegenstand der Anlage

Diese Anlage 1 zum Engineering IT-Rahmenvertrag beschreibt ergänzende Anforderungen und allgemeine Sicherheitsvorkehrungen für den externen Zugriff auf Engineering IT-Applikationen von außerhalb des Betriebsgeländes von Daimler.

2. Allgemeine Anforderungen

2.1 Grundlagen

Engineering IT-Applikationen werden gemäß der darin gespeicherten Daten und Informationen von Daimler nach eigenem Ermessen klassifiziert. Aus dieser Klassifizierung leiten sich insbesondere der Schutzbedarf am externen Arbeitsplatz und die Anforderungen an die Zertifizierung des Auftragnehmers ab (siehe Ziffer 3 dieser Anlage). Die Klassifikationsstufen sind:

- „Öffentlich/public“
- „Intern/internal“
- „Vertraulich/confidential“

2.2 Basis-Anforderungen der IT-Sicherheit

Der Auftragnehmer sorgt dafür, dass auf der für den Zugriff genutzten Hardware ein Virenscanner installiert und regelmäßig aktualisiert sowie das Betriebssystem regelmäßig mit Updates, insbesondere mit Sicherheits-Patches, aktualisiert wird.

Der Auftragnehmer sorgt dafür, dass von Daimler zugeteilte Benutzerkennungen (UserID) und Passwörter nicht an andere als die jeweils konkret damit betrauten Mitarbeiter des Auftragnehmers oder sonstige Dritte weitergegeben werden.

2.3 Security Awareness-Schulung

Der Auftragnehmer sorgt dafür, dass alle mit einem Zugang zu Engineering IT-Applikationen betrauten Mitarbeiter an einer Unterweisung zum Thema „Informationssicherheit für externe Partner“ von Daimler („Security Awareness-Schulung“) teilnehmen.

Die Security Awareness-Schulung ist für jeden Mitarbeiter, der über eine UserID von Daimler verfügt, wie folgt durchzuführen:

- Bei neuen Mitarbeitern spätestens innerhalb der ersten Woche nach Beginn der Tätigkeit.
- Die Schulung ist von jedem Mitarbeiter jährlich zu wiederholen.
- Die Teilnahme ist vom Auftragnehmer zu dokumentieren.

Daimler stellt nach eigenem Ermessen aktuelle Schulungsunterlagen über SupplierPortal/EngineeringService oder das Daimler-Intranet zur Verfügung.

2.4 Audits beim Auftragnehmer

Zur Gewährleistung der Informationssicherheit sind nach ISO 27001 regelmäßige Audits beim Auftragnehmer notwendig. Im Regelfall werden diese per E-Mail angekündigt. Ein Audit beinhaltet folgende wesentliche Schritte, die unter Beachtung von Ziffer 8.4 des Engineering IT-Rahmenvertrages durchgeführt werden:

- Abfrage des aktuellen Status zur IT-Sicherheit beim Auftragnehmer auf Basis der VDA-Checkliste nach VDA ISO 27002:2013.
- Falls der Auftragnehmer bereits nach ISO 27001 zertifiziert ist, genügt die Zusendung des „Statement of Applicability".

Der Zutritt zu folgenden Audit-relevanten Bereichen ist erforderlich:

- Bereiche, in denen Daimler-Informationen verarbeitet werden
- Serverraum/Netzwerk-Aufpunkt der Verbindung zu Daimler
- Allgemeiner Rundgang an der Lokation

2.5 Erstmalige Zugriffe auf Applikationen und Daten

Die erstmalige externe Anbindung eines Auftragnehmers erfordert eine Risikoanalyse durch die IT-Sicherheit von Daimler. Grundlage ist die Erfassung des aktuellen Status zur IT-Sicherheit beim Auftragnehmer auf Basis der VDA-Checkliste nach VDA ISO 27002:2013.

Die vom VDA entwickelte Checkliste zur Überprüfung des vorhandenen Sicherheitsniveaus auf Basis der VDA ISO 27002:2013 ist verfügbar unter:

https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.html

Die Notwendigkeit einer Risikoanalyse besteht unabhängig vom konkreten technischen Zugangsweg. Der jeweilige technische Zugangsweg darf daher nur umgesetzt werden, wenn das Ergebnis der Risikoanalyse der IT-Sicherheit positiv ausfällt.

3. Schutzbedarf

3.1 Klassifikation „Intern“ und „Vertraulich“

Klassifikationsstufe	„Intern/internal“	„Vertraulich/confidential“
Schutzbedarf am Arbeitsplatz	Normaler Arbeitsplatz beim Auftragnehmer (nicht öffentlich zugänglich)	Physisch separierter Bereich mit Sichtschutz
Zertifizierung des Auftragnehmers	Check-Liste	Check-Liste mit Nachweis der Implementierung
Technische Zugangswege	SSL-VPN Always-on IPSec-VPN MPLS ENX	SSL-VPN Always-on IPSec-VPN MPLS ENX
Beispiele	Dialog, SRM, DanTe, Finas, DukE	Smaragd, DOORS
Physischer Schutz	Zutrittsschutz zum Gebäude/Bereich des Auftragnehmers sowie zu den Netzwerkkomponenten (VPN-Box, etc.) Netzwerkkomponenten/Serverraum • Zutrittskontrollsystem (möglichst elektronisch) • Zutritte auf ein notwendiges minimales Maß beschränkt Keine Nutzung in öffentlichen Bereichen (Internetcafé, Flughafen, Bahn, etc.)	Wie bei „Intern“, zusätzlich: Netzwerkkomponenten / Serverraum • Zutrittskontrollsystem (elektronisch) • Tür-Offen-Alarmierung mit maximal 60 Sekunden Verzögerung • Protokollierung der Zutritte Projektbereich mit Sichtschutz (z.B. Milchglasfolie) • Außenfenster, wenn leicht einsehbar • Abtrennung des Projektbereichs, damit unbeteiligte Personen nicht auf die Bildschirme Einsicht bekommen können
Technischer Schutz	• Keine getrennte Infrastruktur notwendig • Netzwerk des Auftragnehmers kann verwendet werden • Zugriffschutz durch Rechtekonzept • Verschlüsselung der Endgeräte (bspw. BitLocker)	• Netzwerk des Auftragnehmers kann verwendet werden • Falls Datenaustausch mit EEW (External Engineering Workplace) möglich: • Eigenes Subnetz zugewiesen • Keine Einbringung von Dritthardware (Systeme, die nicht Daimler oder dem Auftragnehmer gehören) in das spezielle Subnetz • Zugriffschutz durch Rechtekonzept • Datenspeicherung auf separaten Datenspeichern • Verschlüsselung der Endgeräte (bspw. BitLocker)
Organisatorisch	• Security Awareness-Schulung für Mitarbeiter (Begleitung von Fremden im Raum, Datennutzung/Zugriff nur im Rahmen der Beauftragung, etc.)	Wie bei „Intern“, zusätzlich: • Striktes Fotografie-Verbot • Clean Desk Policy • Flächenverantwortlicher ist definiert

3.2 Bei Nutzung von Rohbau-Templates bzw. Gesamtfahrzeug- & DMU-Umfänge

Zusätzlich werden folgende Sicherheitsstandards vorausgesetzt:

- Eigener Projektraum inkl. Zutrittskontrollsystem
- ISO 27002:2013 Zertifizierung
- Separater Netzbereich
- Keine Nutzung von Dritthardware
- Keine ENX und/oder SSL-VPN Verbindungen

3.3 Nutzung der Engineering IT-Applikationen außerhalb des Arbeitsplatzes

Soll die Anbindung an Engineering IT-Applikationen vom Mitarbeiter des Auftragnehmers auch außerhalb des normalen Arbeitsplatzes genutzt werden (z.B. Home Office, Hotelzimmer bei Geschäftsreisen, Versuchsfahrten), so ist dies Daimler vom Auftragnehmer explizit mitzuteilen und bedarf zusätzlich der schriftlichen Einwilligung von Daimler. Die Nutzung in öffentlich zugänglichen Bereichen ist auch in diesem Fall verboten.