# Regelwerk der Informationssicherheit

## Informationssicherheitsregel

# Office-Typen
## (Vorgaben für Räumlichkeiten bei Partneranbindungen)

| | |
|---|---|
| Version | 4.0 |
| Stand: | 02.07.2010 |
| Status: | *freigegeben* |
| Gültig ab: | 12.07.2010 |
| | |
| Ansprechpartner: | W. Vogl, PA-15, R. Schauflinger, FZ-13 |
| Abgestimmt mit: | Hr. Probst, FZ |
| | Hr. Weißhaar, PA-1 |
| | IT-BMK |
| | Netzwerk des Informationsschutzes (DIS) |
| | Netzwerk der IT-Sicherheit (ITSBs) |

# 1 Gegenstand und Geltungsbereich

In dieser Informationssicherheitsregel werden Vorgaben für Räumlichkeiten in der Zusammenarbeit von BMW mit Partnerunternehmen beschrieben, die außerhalb des BMW Werksgeländes liegen und Anbindungen an das BMW Konzernnetz erfordern. In welchen Fällen diese Anforderungen erfüllt werden müssen, ist den Anweisungen zur Informationssicherheit zu entnehmen.

Die Regel gilt für die BMW AG und ihre verbundenen Unternehmen („BMW Group“). Rechtliche Einheiten der BMW Group sind verpflichtet, diese Regel zu übernehmen und anzuwenden, soweit nicht gesetzliche Vorschriften dem entgegenstehen. Falls abweichende lokale Regelungen erforderlich sind, sind diese mit den zuständigen Stellen der Informationssicherheit abzustimmen.

# 2 Überblick über die Office-Typen

Es wird zwischen folgenden Office-Typen unterschieden:

- **Projektbüro**
  Ein Projektbüro bezeichnet ein Büro, das sich nicht auf BMW Gelände befindet und in dem ausschließlich Mitarbeiter eines Partnerunternehmens im Rahmen eines BMW Projektes bzw. im Rahmen von längerfristigen Betriebs- oder Wartungsaufgaben[1] arbeiten.
  Ein Projektbüro ist dann einzurichten, wenn die Kriterien für die Notwendigkeit eines Projektbüros gemäß den Anweisungen zur Informationssicherheit erfüllt sind.

- **Satellitenbüro**
  Ein Satellitenbüro bezeichnet ein Büro, das sich nicht auf BMW Gelände befindet und in dem sowohl Mitarbeiter eines Partnerunternehmens als auch BMW Mitarbeiter im Rahmen von Kooperationsprojekten arbeiten. Ein Satellitenbüro ist dann einzurichten, wenn die Kriterien für die Notwendigkeit eines Satellitenbüros gemäß den Anweisungen zur Informationssicherheit erfüllt sind.

- **Secure-Office**
  Ein Secure Office bezeichnet ein Büro, das sich nicht auf BMW Gelände befindet und zu dem ausschließlich BMW Mitarbeiter Zutrittserlaubnis haben. Ein Secure Office ist dann einzurichten, wenn eine transparente Anbindung an das BMW Konzernnetz benötigt wird.

Die Anforderungen zu den genannten Office-Typen sind in den nachfolgenden Kapiteln im Detail beschrieben.

[1] In den nachfolgenden Kapiteln werden unter *Projekt* auch diese längerfristigen Betriebs- oder Wartungsaufgaben verstanden.

# 3 Anforderungen an ein Projektbüro

### 3.1 Grundsätze

- Die Anweisungen zur Informationssicherheit sind einzuhalten.
- Alle Projekt-Mitarbeiter sind persönlich zur Geheimhaltung zu verpflichten.
- In Projekten, in denen umfangreiche Zugriffe auf Informationen mit besonderem Schutzbedarf existieren (Geheime Projekte, Innovationen, Design-bzw. Konstruktionsdaten in der Konzeptphase oder in der frühen Serienentwicklungsphase) wird eine Zertifizierung nach ISO/IEC 27001 vom Partner gefordert.
  In allen anderen Fällen ist vom Partnerunternehmen auf Verlangen von BMW das Ergebnis einer Selbstauditierung gemäß ISO/IEC 27001 vorzulegen.

### 3.2 Bautechnische Infrastruktur

- Es ist ein eigener Raum mit ausreichendem Sicht-und Mithörschutz vorzusehen.
- Die Hoheit des Projektraums liegt beim Partner (Hausrecht).
- Das Zutrittskontrollsystem muss vom Partner installiert werden und mindestens eine Schlüssellösung umfassen (eigene Schließung, d.h. exklusiver Schlüssel für Projektbüro).
- Der Partner-Gebäudebereich (in dem sich das Projektbüro befindet) muss mit einem Alarmsystem gesichert sein (Alarmverfolgung).

Hinweis:

Ein Projektbüro muss nicht BMW-projektspezifisch unterteilt werden – ein Büro für alle BMW-Projekte genügt.

### 3.3 Organisatorischer Schutz

- Die Verantwortlichkeiten sind zu regeln (Zutrittsschutz, allgemeines Informationsschutzverhalten).
- Die Zutrittsberechtigung wird durch den Partner erteilt, gepflegt und kontrolliert.
- Auf Rechnern des Partners darf ein BMW-Mitarbeiter (z.B. bei Besuch) seine persönlichen BMW-Authentisierungsdaten nicht benutzen. Gleiches gilt auch für externe Mitarbeiter, die im Auftrag von BMW tätig sind, sofern sie Rechte innehaben, die über das Projekt hinausgehen.
- Der Einsatz von mobilen Speichermedien (auch Notebook) ist vom Projektleiter vor Ort genehmigen zu lassen.
- Fax und Drucker müssen innerhalb des Büros und ausschließlich für BMW-Projekte zur Verfügung stehen (Alternative: Ausdrucke sind nur mittels Ausweisleser am Drucker möglich).

### 3.4 Lokales Netzwerk (LAN)

- Es muss ein dediziertes Subnetz für das Projektbüro definiert werden.
- Das Subnetz des Projektbüros muss zwingend physikalisch oder logisch vom lokalen Netzwerk des Partners getrennt sein.

- Für das Subnetz sind entweder offizielle IP-Adressen vom Partner zur Verfügung zu stellen oder von BMW vergebene private IP-Adressen zu verwenden.
- Eine IP-Adressumsetzung (NAT) am Übergang zum Projektbüro darf nicht erfolgen.
- Die aktiven Netzwerkkomponenten sind in einem abschließbaren EDV-Schrank aufzustellen – Zugang ist nur für die Systemverantwortlichen erlaubt.

Hinweis:

Wird eine logische Trennung gewählt, muss eine Netzwerkabsicherung des Projektbüros gegenüber dem lokalen Netzwerk des Partners vorhanden sein, z. B. durch eine Firewall.

### 3.5 Anbindung an das BMW Konzernnetz (Zuliefererанbindung; WAN)

- Den externen Partnern steht nur ein selektiver Zugriff zu den BMW Systemen im Konzernnetz zur Verfügung. Zugriffe auf schützenswerte BMW Systeme müssen explizit freigegeben werden.
- Sofern der WAN-Übergabepunkt nicht im Projektbüro liegt, muss die Kommunikation über das Partnernetzwerk verschlüsselt erfolgen.

### 3.6 Anbindung an andere Netze

- Der Zugriff vom Partnernetz oder einem Netz außerhalb des Partnernetzes in das Projektbüro ist grundsätzlich verboten. Einzige Ausnahme ist die Remote Administration der IT-Infrastruktur des Partners im Projektbüro und der Anschluss von Telearbeitsplätzen für Partnermitarbeiter. Die Rahmenbedingungen hierzu müssen eingehalten werden, siehe Kapitel 6.
- Der Netzwerkübergang zum Projektbüro ist zu dokumentieren und BMW auf Verlangen vorzulegen.
- Die Anbindung eines Projektbüros an ein anderes BMW Projektbüro ist zulässig, sofern die jeweils benötigten BMW Freischaltungen gleich sind.

### 3.7 Software und Applikationen

- Auf den Endgeräten (Desktop, Laptop, …) im Projektbüro darf nur die für den Projektumfang notwendige Software installiert sein. Ein BMW Group Client (Standardinstallation für interne BMW Clients) ist nicht erlaubt.
- Sofern auch Applikationen und Systeme des Partners genutzt werden, muss ein angemessener Schutz der BMW-relevanten Daten in diesen Applikationen und Systemen sichergestellt sein (u. a. Datensegmentierung mindestens auf Ebene der beteiligten Partnerfirmen, sichere Authentisierung, Rechte und Rollen, gesicherte Datenhaltung und –übertragung).

### 3.8 Hardware

- Externen Partnern wird empfohlen, die Hardware nach dem BMW Blueprint Standard auszuwählen.

### 3.9 Systemadministration

- Die IT-Infrastruktur (Endgeräte, Server, Netzwerkkomponenten) des Partners ist vom Partner zu betreuen.

- Es muss gewährleistet sein, dass ein aktueller Virenschutz installiert ist und sichere Betriebssystem-Release-Stände eingespielt sind.

### 3.10 Security-Audits

Die Partnerfirma muss BMW ermöglichen, die Einhaltung der BMW Vorgaben vor Ort zu überprüfen.

# 4 Anforderungen an ein Satellitenbüro

### 4.1 Grundsätze

- Die Anweisungen zur Informationssicherheit sind einzuhalten.
- Alle Projekt-Mitarbeiter sind persönlich zur Geheimhaltung zu verpflichten.
- In Projekten, in denen umfangreiche Zugriffe auf Informationen mit besonderem Schutzbedarf existieren (Geheime Projekte, Innovationen, Design-bzw. Konstruktionsdaten in der Konzeptphase oder in der frühen Serienentwicklungsphase) wird eine Zertifizierung nach ISO/IEC 27001 vom Partner gefordert. Beispiel: Kooperationsprojekte.
  In allen anderen Fällen ist vom Partnerunternehmen auf Verlangen von BMW das Ergebnis einer Selbstauditierung gemäß ISO/IEC 27001 vorzulegen.

### 4.2 Bautechnische Infrastruktur

- Es ist ein eigener Raum mit ausreichendem Sicht-und Mithörschutz vorzusehen.
- Sofern BMW die Hoheit über das Satellitenbüro hat, ist das BMW-Standard-Zutrittskontrollsystem (Ausweisleser) zwingend. Falls der Partner die Hoheit hat, muss er ein Zutrittskontrollsystem installieren, das vergleichbar mit dem BMW-Standard ist.
- Das Büro muss alarmgesichert sein (entweder durch direkte Alarmsicherung des Büros oder durch Alarmsicherung der Partnerlokation).

### 4.3 Organisatorischer Schutz

- Die Verantwortlichkeiten sind zu regeln (Zutrittsschutz, allgemeines Informationsschutz-Verhalten).
- Die Hoheit für das Büro kann bei BMW oder beim Partnerunternehmen liegen.
- Sofern BMW im Satellitenbüro die Hoheit hat, wird die Zutrittsberechtigung durch die BMW Fachabteilung erteilt, gepflegt und kontrolliert. Sofern der Partner die Hoheit hat, muss BMW zumindest eine Kontrollmöglichkeit (z.B. Begehung mit Überprüfung vor Ort) eingeräumt werden.
- Auf Rechnern des Partners darf ein BMW-Mitarbeiter seine persönlichen BMW-Zugangsdaten (UserID/Passwort) nicht benutzen. Gleiches gilt auch für externe Mitarbeiter, die im Auftrag von BMW tätig sind, sofern sie Rechte innehaben, die über das Kooperationsprojekt hinausgehen.
- Das sichtbare Tragen des Firmenausweises ist obligatorisch.
- Der Einsatz von mobilen Speichermedien (auch Notebook) ist vom Projektleiter vor Ort genehmigen zu lassen.
- Fax und Drucker müssen innerhalb des Büros stehen. Drucker dürfen vom BMW Konzernnetz aus nicht ansprechbar sein, sofern kein weiterer Schutz aktiviert ist (Alternative: Ausdrucke sind nur mittels Ausweisleser am Drucker möglich).

### 4.4 Lokales Netzwerk (LAN)

- Es muss ein dediziertes Subnetz für das Satellitenbüro definiert werden.
- Das Subnetz des Satellitenbüros muss zwingend physikalisch oder logisch vom lokalen Netzwerk des Partners getrennt sein.

- Für das Subnetz sind entweder offizielle IP-Adressen vom Partner zur Verfügung zu stellen oder von BMW vergebene private IP-Adressen zu verwenden.
- Eine IP-Adressübersetzung (NAT) am Übergang zum Satellitenbüro darf nicht erfolgen.
- Die aktiven Netzwerkkomponenten sind in einem abschließbaren EDV-Schrank aufzustellen – Zugang ist nur für die Systemverantwortlichen erlaubt.

Hinweis:

- Wird eine logische Trennung gewählt, muss eine Netzwerkabsicherung des Satellitenbüros gegenüber dem lokalen Netzwerk des Partners vorhanden sein, z. B. durch eine Firewall.

### 4.5 Anbindung an das BMW Konzernnetz (Zuliefererанbindung; WAN)

- Den BMW Mitarbeitern muss ein transparenter Zugriff auf das BMW Konzernnetz (z.B. mittels VPN) ermöglicht werden.
- Den externen Partnern steht nur ein selektiver Zugriff zu den BMW Systemen im BMW Konzernnetz zur Verfügung.
- Sofern der WAN-Übergabepunkt nicht im Satellitenbüro liegt, muss die Kommunikation über das Partnernetzwerk verschlüsselt erfolgen.

### 4.6 Anbindung an andere Netze

- Der Zugriff vom Partnernetz oder einem Netz außerhalb des Partnernetzes in das Satellitenbüro ist grundsätzlich verboten. Einzige Ausnahme ist die Remote Administration der IT-Infrastruktur des Partners im Satellitenbüro und der Anschluss von Telearbeitsplätzen für Partnermitarbeiter. Die Rahmenbedingungen hierzu müssen eingehalten werden, siehe Kapitel 6.
- Der Netzwerkübergang zum Satellitenbüro ist zu dokumentieren und auf Verlangen BMW vorzulegen.
- Die Anbindung eines Satellitenbüros an ein anderes Satellitenbüro ist zulässig, sofern die jeweils benötigten BMW Freischaltungen gleich sind und insbesondere die physikalische bzw. logische Trennung vom lokalen Netzwerk des Partners sicher gestellt ist.

### 4.7 Software und Applikationen

- Der Zugriff auf das BMW Konzernnetz bzw. auf BMW Applikationen darf nur mittels freigegebener Software (Blueprint) von BMW erfolgen.
- Sofern auch Applikationen und Systeme des Partners genutzt werden, muss in diesen Applikationen und Systemen ein angemessener Schutz der BMW-relevanten Daten sichergestellt sein (u. a. Datensegmentierung mindestens auf Ebene der beteiligten Partnerfirmen, sichere Authentisierung, Rechte und Rollen, gesicherte Datenhaltung und –übertragung).

### 4.8 Hardware

Externen Partnern wird empfohlen, die Hardware nach dem BMW Blueprint Standard auszuwählen.

### 4.9 Systemadministration

- Die BMW IT-Infrastruktur (Endgeräte, Server, Netzwerkkomponenten) ist von BMW zu betreuen.
- Die Partner IT-Infrastruktur muss vom Partner betreut werden.
- Es muss gewährleistet sein, dass ein aktueller Virenschutz installiert ist und sichere Betriebssystem-Release-Stände eingespielt sind.
- Wird eine Firewall zwischen dem lokalen Netzwerk des Partners und dem Subnetz des Satellitenbüros eingesetzt, so muss die Konfiguration und Administration der Firewall
    - entweder durch BMW erfolgen
    - oder vertraglich geregelt werden.

### 4.10 Security-Audits

Sofern die Verantwortung für das Satellitenbüro bei der Partnerfirma liegt, muss die Partnerfirma BMW ermöglichen, die Einhaltung der BMW Vorgaben vor Ort zu überprüfen.

# 5 Anforderungen an ein Secure-Office

### 5.1 Grundsätze

- Die Anweisungen zur Informationssicherheit sind einzuhalten.

### 5.2 Bautechnische Infrastruktur

- Es ist ein eigener Raum mit ausreichendem Sicht-und Mithörschutz vorzusehen.
- Die Hoheit über das Secure-Office muss auf BMW übertragen werden (z.B. Schlüsselübergabe, Versiegelung von Türen, etc.).
- Das BMW-Standard-Zutrittskontrollsystem ist zwingend (Ausweisleser oder Schlüssellösung, falls die Anzahl der Zutrittsberechtigungen sehr gering ist).
- Das Büro muss alarmgesichert und mit einer Alarmverfolgung ausgestattet sein.

### 5.3 Organisatorischer Schutz

- Die Verantwortlichkeiten sind zu regeln (Zutrittsschutz, allgemeines Informationsschutz-Verhalten).
- Die Zutrittsberechtigung wird durch die BMW Fachabteilung erteilt, gepflegt und kontrolliert.
- Das sichtbare Tragen des Firmenausweises ist obligatorisch.
- Fax und Drucker müssen innerhalb des Büros stehen.

### 5.4 Lokales Netzwerk (LAN)

- Es muss ein dediziertes Subnetz für das Secure-Office definiert werden.
- Das Subnetz muss zwingend physikalisch oder logisch vom lokalen Netzwerk des Partners getrennt sein. Für die logische Trennung ist eine Netzwerkabsicherung (z.B. durch eine Firewall) zwingend.
- Die IP-Adressen für das Subnetz sind von BMW zur Verfügung zu stellen.
- Alle aktiven Netzwerkkomponenten müssen in einem abschließbaren EDV-Schrank innerhalb des Secure-Office stehen.

### 5.5 Anbindung an das BMW Konzernnetz (Zuliefererанbindung; WAN)

- Der Zugriff aus dem Secure-Office in das BMW Konzernnetz ist so zu konfigurieren, dass er transparent ist.
- Der WAN-Übergabepunkt muss entweder im Secure-Office liegen oder es muss eine verschlüsselte Verbindung in das Secure-Office gewährleistet sein.

### 5.6 Software

- Nur von BMW durch das Blueprint-Verfahren zugelassene Software ist erlaubt.
- Nur der BMW Group Client ist erlaubt.

### 5.7 Hardware

Der BMW-Standard ist obligatorisch.

### 5.8 Systemadministration

Die IT-Infrastruktur (Endgeräte, Server, Netzwerkkomponenten) wird von BMW betreut.

### 5.9 Security-Audits

Die Auditierung der korrekten Umsetzung dieser Vorgaben liegt in der Verantwortung der BMW Fachbereiche.

Die Stellen der Sicherheit (Informationsschutz, IT-Sicherheit) sind berechtigt, die Unterlagen einzusehen und die Maßnahmen zu überprüfen.

# 6 Anhang

### 6.1 Definition der Benutzergruppen

- BMW Mitarbeiter
    - Zutritt zu allen vorgesehenen Büroflächen.
    - Zugriff auf alle für seine Tätigkeiten benötigten projektrelevanten Daten im Rahmen seines Arbeitsvertrags.
    - Transparenter Zugriff auf das BMW Konzernnetz.
- Externer Mitarbeiter / Fremdkraft
    - Keine Zutrittsberechtigung zum BMW Secure-Office (Zutritt in Begleitung eines BMW Mitarbeiters ist aber möglich).
    - Zugriff auf alle für seine Tätigkeiten benötigten projektrelevanten Daten.

### 6.2 Rahmenbedingungen zur Remote Administration der IT-Infrastruktur des Partners in Projekt- oder Satellitenbüros durch den Partner

#### 6.2.1 Organisatorische Ebene

- Der Zugang zur IT-Infrastruktur ist dediziert zu regeln.
- Der autorisierte Remote Administrator muss eine Geheimhaltungsverpflichtung unterschreiben.
- Es muss sichergestellt sein, dass nur die namentlich festgelegten Administratoren auf die IT-Systeme zugreifen können. Die Namen der Systemadministratoren müssen BMW auf Verlangen offen gelegt werden.

#### 6.2.2 Systemebene

- Remote-Zugang zum Projektbüro ist nur temporär, überwacht und ausschließlich für Wartungs-und Administrationsarbeiten zulässig.
- Für die Remote Administration ist starke Authentisierung erforderlich (besteht aus Wissen und Besitz, z.B. UserID/Passwort und SecurID).
- Die Remote Administration muss mitprotokolliert werden und das Protokoll auf Verlangen BMW zur Verfügung gestellt werden.

#### 6.2.3 Netzwerkebene

- Während der Administration darf die Administrationskonsole nur mit dem Netzwerk des Projekt- oder Satellitenbüros verbunden sein.
    - Eine verschlüsselte Verbindung zwischen der Administrationskonsole und dem Projektbüro ist notwendig.

### 6.3 Sonderregelung zur Anbindung von Telearbeitsplätzen

#### 6.3.1 Organisatorische Ebene

Es muss sichergestellt werden, dass von einem Telearbeitsplatz aus ausschließlich als Projektmitarbeiter ausgewiesene Mitarbeiter des Partnerunternehmens, die überwiegend im Projekt- oder Satellitenbüro arbeiten, auf das Projekt- oder Satellitenbüro zugreifen können.

#### 6.3.2 Netzwerk-/Systemebene

- Sofern die Telearbeitsverbindung nicht direkt im Projekt- oder Satellitenbüro terminiert, muss sichergestellt werden, dass die Kommunikation über das Partnernetzwerk verschlüsselt erfolgt.
- Der Zugriff von Telearbeitsplätzen auf das Projekt- oder Satellitenbüro muss durch eine starke Authentisierungslösung (besteht aus Wissen und Besitz, z.B. UserID/Passwort und SecurID) abgesichert sein.
- Die Lösung für Telearbeitsplätze des Partnerunternehmens muss bzgl. Sicherheit mit einer BMW Lösung vergleichbar sein (z.B. Vorhandensein einer Personal Firewall, Nutzung sicherer Verschlüsselungsalgorithmen, Schutz vor so genanntem Split Tunneling).