# Cooperation with partners

## Requirements of a project office

BMW Group

# Requirements an a project office with external partners

(Project office staffed by only partner employees)

## Principles

- The secrecy is regulated between the partners in the contract and is agreed.
- All employees are to be obliged personally to the secrecy.
- Orientation on standard ISO/IEC 27001 respectively 17799 (VDA-Recommendation on May, 2005).

## Structural engineering infrastructure

- Defined, separate room required with protection from others listening or seeing in.
- The partner retains sovereignty of the project room (right of possession).
- The access control system is installed by the partner (key solution as a minimum).
- The partner's area of the building is secured by an alarm (monitoring).

## Note:

- A project office does not have to be BMW project-specific partitioned – one office for all BMW projects is adequate.

## Organisational protection

- Responsibilities are to be regulated (IPD, PM).
- Access authorisation is administered and controlled by the partner.
- To use his personal BMW authentication data on partner hardware is not allowed for BMW employees. Same for the external employees, which are working by order of BMW  if they have rights, that exceed  the project scope.
- Confidential data has to be archieved saved for access on the hard disk.
- Strictly confidential data has to be archieved encrypted, in case unauthorized access is possible (e. g. hard disk of a laptop)
- Usage of mobile storage media (including laptop computers) is to be approved by the PM (SM).
- Fax machines and printers must be positioned within the office.

IPD = Information Protection Delegate
PM =  Project Manager
SM =  Senior Manager

# Requirements an a project office with external partners

(Project office staffed by only partner employees)

## Network (LAN)

- Physical or logical separation from the partner's LAN is mandatory.
- Official IP addresses are provided by the partner. (Alternatively: BMW provides IP addresses in accordance with RFC1918 172.16.0.0/12, 192.168/16)
- NAT (Network Address Translation) of partner IP addresses to the IP ranges of the project office is not permitted!
- Active network components are located in a lockable IT cabinet - only system managers have access.

## Connection to other networks

- Access from the partner's network into the project office is generally forbidden. The sole exception is the remote administration of the IT equipment in the project office.
- Network transitions to the partner's office are to be documented and presented to BMW upon request.
- General conditions on remote administration must be satisfied, refer to the last slide.

## Network (supplier connection; WAN)

- Only a selective access to the BMW application software in the BMW Corporate Network (CN) is available to external partners.
- If the WAN transfer point lies outside of the project office, it must be guaranteed that the data traffic between the project office and WAN transfer point can NOT be "bugged".

## Note:

- Encoding can only be performed at the software application level and cannot currently be provided at network level except for the BMW VPN client.

# Requirements an a project office with external partners

(Project office staffed by only partner employees)

## Software

- Only the software required for the scope of the project may be installed on the computers. A BMW enterprise client (sample client for internal BMW employees) is not permitted.
- Should the partner's application software programs and systems be used, an appropriate protection of BMW-relevant data must be ensured in these programs and systems (including data segmentation at least on the level of involved partner companies, secure authentication, rights and roles, secured data management and transmission)

## Hardware

- It is recommended to external partners that they select hardware according to the BMW Blueprint Standard.

## System administration

- The partner's infrastructure (computers, servers, IT equipment / network components) is maintained by the partner.
- It must be guaranteed that current virus signatures and secure OS release versions are applied.

## Security audit

- The requirement for an audit is analysed according to the BMW evaluation scheme.
- The audit is carried out by accredited service providers.

# General conditions on remote administration of IT equipment in project offices by the partner

## Organisational level

- Remote access to the project office or satellite office is monitored only non-permanently and is permissible exclusively for maintenance and administration tasks.
- Access to administrable IT equipment is to be regulated as being dedicated.
- The authorised remote administrator must sign an obligation to maintain secrecy.

## System level

- Strong authentication (knowledge + ownership, e.g. UserId/password + SecureID) is required for remote administration.
- Remote administration must be logged, and the log must be made available to BMW upon request.
- Remote access is only temporary, monitored and exclusive for maintenance- and administrationoperations allowed.

## Network level

- The administration console may only be connected to the project office network whenever adminstration is being carried out.
- A connection secured against eavesdropping is necessary between the administration console and the project office.