**IT Emergency Handbook  
(IT Disaster Recovery Manual)**

**for Plant 52.10 – Araquari**

# Document Steering Information

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **BMW Group** | **Document class**: 3.2 | | | | **Doc.-No.:** <optional> | |
| **Range of validity**: BMW Group Brazil | | | | **Version**: V1 | |
| **IT Emergency Handbook for Plant 52.10 (Araquari) 2024** | | | | **Status**:  <Draft> | |
|  | **Coordinated with (person, dept, circle):** | | | | Gabriel Sutil, FG-AM-44 | |
|  | | | | | | |
| **Change history** | | | | | | |
| **Version** | | **Content of changes** | **Written by**  **Dept Code**  **Date** | **Reviewed by**  **Dept Code**  **Date** | | **Released by**  **Dept Code**  **Date** |
| 1 | | Update Template | FG-AM-44  Sep 22nd, 2023 | FG-AM-44  Sep 22nd, 2023 | | FG-AM-44  Sep 22nd, 2023 |
|  | |  |  |  | |  |
|  | |  |  |  | |  |
|  | |  |  |  | |  |

**List of important links:**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Link** | **Comment** |
| IT Crisis Management | <http://itcm.bmwgroup.net/> | confluence page incl. escalation numbers |

Table of Content

[Document Steering Information 2](#_Toc150247614)

[1. Introduction 6](#_Toc150247615)

[1.1. Security Guidelines 6](#_Toc150247616)

[1.2. Validity of this Handbook 6](#_Toc150247617)

[1.3. Distribution list 7](#_Toc150247618)

[1.4. Purpose of the IT Emergency Handbook 8](#_Toc150247619)

[1.5. Updates and Changes 9](#_Toc150247620)

[1.6. IT Emergency Handbook and Related Documentation 10](#_Toc150247621)

[2. IT Emergency Management 11](#_Toc150247622)

[2.1. Organisational structure 11](#_Toc150247623)

[2.1.1. Involvement and Roles 11](#_Toc150247624)

[2.1.2. IT Emergency Management Team: roles, tasks and responsibilities 14](#_Toc150247625)

[2.1.3. IT Emergency Management Team: Contact data 15](#_Toc150247626)

[2.1.4. Process flow 15](#_Toc150247627)

[2.1.5. Escalation strategy 15](#_Toc150247628)

[2.2. Dealing with used forms 15](#_Toc150247629)

[3. Scenarios and Recovery Procedures 16](#_Toc150247630)

[3.1. Scenarios 16](#_Toc150247631)

[3.1.1. Trigger Scenarios (also: Contingency Scenarios) 16](#_Toc150247632)

[3.1.1.1. Definition 16](#_Toc150247633)

[3.1.1.2. Reference Documentation 16](#_Toc150247634)

[3.1.2. IT Outage Scenarios (also: Disaster or Failure Scenarios) 17](#_Toc150247635)

[3.1.2.1. Definition 17](#_Toc150247636)

[3.1.2.2. Description of Scenario: Outage of NCC1 - Araquari W52.10 (52.10/001.0/00.0/012) 17](#_Toc150247637)

[3.1.2.3. Description of Scenario: Outage of room NCC2 - Araquari W52.10 (52.10/050.0/00.0/403) 19](#_Toc150247638)

[3.2. Recovery Procedures 20](#_Toc150247639)

[3.2.1. Overview 20](#_Toc150247640)

[3.2.2. Recovery Strategy 21](#_Toc150247641)

[3.2.3. Recovery procedures for Scenario Room NCC1 - Araquari W52.10 (52.10/001.0/00.0/012) 22](#_Toc150247642)

[3.2.4. Recovery procedures for Scenario Room NCC2 - Araquari W52.10 (52.10/050.0/00.0/403) 23](#_Toc150247643)

[4. Attachments 24](#_Toc150247644)

[4.1. IT Resources 24](#_Toc150247645)

[4.2. List of abbreviations 25](#_Toc150247646)

[4.3. Layouts 26](#_Toc150247647)

[4.3.1. Data Center in building 52.10/001.0/00.0/012 26](#_Toc150247648)

[4.3.2. Data Center in building 52.10/050.0/00.0/403 26](#_Toc150247649)

[5. TEMPLATE Steering Information 27](#_Toc150247650)

# Introduction

## Security Guidelines

Employees may only be granted access to this document when they require the information to perform their assigned tasks, duties or functions.

## Validity of this Handbook

This Handbook is valid for **Plant 52.10 – Araquari**. Any content of this Handbook does relate to **Plant 52.10 – Araquari** unless stated otherwise.

**Acceptance of the current IT Emergency Handbook**

This handbook has been reviewed, verified and accepted by local IT management:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Frank Schwanz, Local IT Manager FG-AM-44

## Distribution list

| **Name** | **Function(s)** |
| --- | --- |
| Escalation Manager, Greg Marler, FG-AM-4 [Greg.Marler@bmwgroup.com](mailto:Greg.Marler@bmwgroup.com) | IT Director – [FG-AM-4] |
| Escalation Manager, Schwanz Frank, FG-AM-44 [frank.schwanz@bmwgroup.com](mailto:frank.schwanz@bmwgroup.com)  +55 47 99182-5330 | IT Team Manager Brazil- [FG-AM-44] |
| IRE Americas, Ethel Mason Berg, FG-AM-8 [Ethel.Mason-Berg@bmwgroup.com](mailto:Ethel.Mason-Berg@bmwgroup.com) | IRE for Region Americas and Plant Spartanburg |
| LRE Americas, Harding Alan, FG-AM-4 [Alan.Harding@bmwgroup.com](mailto:Alan.Harding@bmwgroup.com) | LRE for Region Americas and Plant Spartanburg |
| IRE LATAM, Altamirano Rodrigo, FG-AM-82 [Rodrigo.Altamirano@bmw.com.mx](mailto:Rodrigo.Altamirano@bmw.com.mx)  +524441418644 | IT Manager Infrastructure Technology - [FG-AM-82] |
| IRE/OE, Sutil Gabriel, FG-AM-44 [Gabriel.Sutil@bmw.com.br](mailto:Gabriel.Sutil@bmw.com.br)  +55 47 99230-4479 | IaaS/Cybersecurity Analyst Araquari - [FG-AM-44] |
| LRE/OE, Suelem Oliboni, FG-AM-44 [Suelem.Oliboni@bmw.com.br](mailto:Suelem.Oliboni@bmw.com.br)  +55 47 99251-1607 | IT Operations Analyst Araquari - [FG-AM-44] |
| Network, Fogaca de Azevedo Moises, FG-AM-44 [Moises.A.Fogaca@bmw.com.br](mailto:Moises.A.Fogaca@bmw.com.br)  +55 47 99226-2181 | Connectivity Analyst Araquari- [FG-AM-44] |
| Workplace, Lucoli Deyvis, FG-AM-44 [Deyvis.Lucoli@bmw.com.br](mailto:Deyvis.Lucoli@bmw.com.br)  +55 47 99201-0929 | Workplace Analyst Araquari- [FG-AM-44] |
| Escalation Manager, Goddard Geoff, FG-AM-8 [Geoff.Goddard@bmwgroup.com](mailto:Geoff.Goddard@bmwgroup.com)  +1-864-450-7684 | IT Director– [FG-AM-8] |
| Escalation Manager, Troisi Chris, FG-AM-83 [Christopher.Troisi@bmwmc.com](mailto:Christopher.Troisi@bmwmc.com) | IT Team Manager – [FG-AM-83] |
| Local MIM | +55 47 3016-1400 |
| Server Operations (P10) MOD | +1-864-802-4405 |
| Datacenter MOD (Americas) | +1-864-802-3154 |

## Purpose of the IT Emergency Handbook

|  |  |
| --- | --- |
| This handbook describes the procedures for the recovery from an IT disaster.  All recovery procedures are derived from defined IT outage scenarios. | **Preamble** |
|  |  |
| The use of this manual is mandatory in the case of an IT Crisis / IT disaster. The procedures must be applied consistently and the defined practices carried out as stated.  For all other cases the procedures of Incident Management Process are applicable.  In case of an IT Crisis all activities must be coordinated with the IT Crisis Management Team. | **Imperative** |
|  |  |
| Critical information which is necessary to recover IT operations and/or deal with IT emergency situations according to the agreed timescales, such as:  General IT Emergency Management approach  IT Disaster Scenarios  IT Disaster Recovery Procedures  Roles and functions necessary to perform IT Disaster Recovery  Interface to IT Crisis Management  Important Note:  Due to the close interaction between IT Crisis Management and IT Disaster Recovery activities it is mandatory that this IT Emergency Handbook is conjunct with local Emergency Management and central IT Crisis Management procedures and manuals. | **Scope** |

Especially for Alarm and Escalation Plans (i.e. initiation of teams for DR) it is strongly recommended to use the mechanisms and tools of IT Crisis Management!  
(ECM and FACT24, both provided by the ITSCM process owner, see also [*http://itcm.bmwgroup.net/*](http://itcm.bmwgroup.net/)

|  |  |
| --- | --- |
| Out of the scope for this manual are:  Pandemic Scenarios  Business interim procedures  Recovery procedures on application level (Documented in App operations manual) | **Out of Scope** |

## Updates and Changes

**Procedure**

* Updates to the IT Emergency Handbook are published at least at 12-monthly intervals or in case of demand. The changes or additions are noted in the change list.
* If there are no changes pending when the manual comes up for re-publication, the chapter “Change List” has to be updated with the entry “No changes”.
* Triggered by the LRE/IRE/OE, every 12 months the manual is reviewed by local IT management to decide whether it is up to date or not. A written report is made of the findings and a note entered in the change list of the completed DR Manual review. The copies held in stock should be updated following the review.
* The new changes are entered in a copy of the IT Emergency Handbook and the version number incremented.  
  The media with the IT Emergency Handbook (current version) is kept in the IT Emergency Management Team's emergency rooms.

**Editorial Responsibility**

Overall responsibility for contents and acceptance from local IT management is incumbent on the LRE/IRE/OE.

The members of Operations Team (DevOps team) and/or local ITSCM team account for the single topics within the manual.

Editorial staff:

|  |  |
| --- | --- |
| ITSCM Process Owner | Dreher, Christian, FG-861 |
| member IaaS/Cybersecurity | Sutil, Gabriel, FG-AM-44 |
| member network, telecoms | Fogaca, Moises, FG-AM-44 |
| member workplace solutions | Lucoli, Deyvis, FG-AM-44 |
| member IT Crisis Management | Schwanz, Frank, FG-AM-44 |
| IRE | Mason Berg, Ethel, FG-AM-8 |
| IRE/OE | Altamirano, Rodrigo, FG-AM-82 |
| IRE/OE | Sutil, Gabriel, FG-AM-44 |
| LRE | Harding, Alan, FG-AM-4 |
| LRE/OE | Oliboni, Suelem, FG-AM-44 |

## IT Emergency Handbook and Related Documentation

Information on items such as superordinate (IT) Crisis Management structures, codes of practice, alarm and escalation procedures, or technical instructions for the single IT infrastructure components, etc. are defined and described in **separate manuals and policies**.

The IT Emergency Handbook should therefore always be used in conjunction with the following documentation:

**Central IT Crisis Management Handbook (**[*http://itcm.bmwgroup.net/*](http://itcm.bmwgroup.net/) **)**

The IT Crisis Management Handbook is the responsibility of ITSCM process owner and deals with central IT Crisis Management (BMW Group-wide).

The manual describes all instances, roles and responsible stakeholders in central IT Crisis Management, the alarm and escalation strategies, authorities and responsibilities in the event of a crisis, criteria for an IT crisis and further more.

In the event of an IT crisis, all activities should be liaised with the central IT Crisis Management Team as appropriate.

**Policies of the local Operational Catastrophe Protection Organisation  
(Betriebliche Katastrophenschutzorganisation, BKO)**

Severe incidents with a threat to life and limb, the environment, or valuable business equipment, have to be combated by a concerted effort with a unified steering team. To ensure efforts stay focused, IT Emergency Management must follow the codes of practice of the local Operational Catastrophe Protection Organisation (OCP) or similar organisation on site.

**IT Operating Manuals / User Manuals**

In these manuals, all procedures for operating, maintaining and recovering IT infrastructure and applications are described. If appropriate, they can be referenced within DR procedures (recommended).

# IT Emergency Management

The IT Emergency Management is part of the global IT Crisis Management process. IT Emergency Management treats of location-specific roles and procedures to cope with an IT Crisis and can as well be used for IT Emergency situations at this location that requires gathering a team of specialists and managers.

The global IT Crisis Management process is defined and approved. You can find the current handbook, references and further explanation on the IT Crisis Management homepage in the intranet: [*http://itcm.bmwgroup.net/*](http://itcm.bmwgroup.net/) .

All information in this chapter is to be adapted to exisiting organisational and procedural surroundings.

### IT Emergency Management Team: Contact data

The contact data for the IT Emergency Management Team can be found here:

<https://contenthub-de.bmwgroup.net/web/it/americas/itpa/team>

### Process flow

The process flow is equal to the definition "Procedure of Major Incidents (MIM Process)" that can be found on the Incident Management intranet pages.

Link: <http://im.bmwgroup.net> 🡺 Documents 🡺 Major Incident Manager

### Escalation strategy

The Escalation stages that are included in the "Procedure of Major Incidents (MIM Process)" are valid accordingly.

## Dealing with used forms

All kinds of used forms and written notes relating to an IT Crisis or an IT Emergency have to be collected for later analysis.

Responsible:

LRE/IRE/OE

# Scenarios and Recovery Procedures

## Scenarios

### Trigger Scenarios (also: Contingency Scenarios)

#### Definition

The triggers of IT emergency situations are described in Trigger Scenarios. They are possible causes for Outage Scenarios and IT Emergency or IT Crisis situations, respectively.

Trigger Scenarios

* **Failure** - Power / Network / Human Resources / Hardware, Denial of access to a building,
* **Destruction** - Natural Disasters / Fire / Water / Flood (Geographical Impact) / physical aggression / Data Centre Gas suppression failure, Terrorist attack
* **Corruption** (IT Security) - Ransomware and other Cyberattacks / Data Privacy / Corruption of Data

**An IT Disaster Scenario / IT crisis can have the following causes:**

* Power / Utility Outage (Complete or Partial)
* Data corruption / Data Loss
* Ransomware and other Cyberattacks
* Hardware Failure / Destruction
* Network Interruptions and outages

**The underlying causes and the first responses in each case to an emergency or crisis situation are not dealt with in any detail in this IT Emergency Handbook.**

#### Reference Documentation

The following reference documentation has the purpose of describing these causes and how to respond to them. These documents are kept up-to-date by designated functional units:

* Major Incident Management - <https://atc.bmwgroup.net/confluence/display/RELOPS/%5BRELOPS%5D+Major+Incident+Management>
* Problem Management Process -   
  <https://atc.bmwgroup.net/confluence/display/RELOPS/%5BRELOPS%5D+Manage+Problems>

### IT Outage Scenarios (also: Disaster or Failure Scenarios)

#### Definition

An Outage Scenario describes as accurately as possible which IT infrastructure components (and ideally applications) are no longer available following a defined incident (e.g. failure of a complete IT room / building / service…).  
Outage Scenarios are caused by Trigger Scenarios. From each Outage Scenario an IT Disaster Recovery Procedure has to be derived.

Identify possible Trigger Scenarios 🡪 Identify relevant Disaster Scenarios 🡪 Define recovery procedures

Resources and planning guides can be found on the ITSCM page: [*http://itcm.bmwgroup.net/*](http://itcm.bmwgroup.net/)

The following IT Disaster Scenarios are taken into account within this handbook:

#### Description of Scenario: Outage of NCC1 - Araquari W52.10 (52.10/001.0/00.0/012)

|  |  |
| --- | --- |
| ***Scenario*** | ***Effects on IT Operations*** |
| Total unavailability of NCC1 (52.10/001.0/00.0/012) due to power outage. | Complete loss of Server Room 52.10/001.0/00.0/012 and Network Room 52.10/001.0/00.0/012.  All IT Services (based on the local IT infrastructure) hosted in Server Room 52.10/001.0/00.0/012 are unreachable. No network connections on Administrative building (52.10/001.0) since wired and wireless connections are connected to the access switch inside the NCC1.  Public telephony services (inbound and outbound calls) are offline.  Switchover of all Network access to NCC2 (52.10/050.0/00.0/403).  All locally hosted applications are temporarily or permanently lost. |
| ***List of applications*** | |
| |  |  |  | | --- | --- | --- | | **Appl ID** | **Application** | **Criticality** | | APPD-169296 | ASBC PKI BR PROD | High Critical (HC) | | APPD-15155 | Cascade P52.10 Brasilien PROD | High Critical (HC) | | APPD-67836 | HEAT Client Management PROD | High Critical (HC) | | APPD-02280 | Infrastructure Service Active Directory Domain Services (AD DS) PROD | High Critical (HC) | | APPD-03544 | Infrastructure Service Server Virtualization PROD | High Critical (HC) | | APPD-238687 | Infrastructure Service SQL Server 2019 App Server PROD | High Critical (HC) | | APPD-238637 | Infrastructure Service SQL Server 2019 PROD | High Critical (HC) | | APPD-00690 | BRiAN PROD | Critical (C) | | APPD-15678 | INIS Americas Prod (ISPI Next Internal Server) | Critical (C) | | APPD-17546 | IPS-PPZ;P52 PROD | Critical (C) | | APPD-248417 | PureConnect Contact Center Americas (PROD) | Critical (C) | | APPD-185864 | SCCM 2012 Prod | Critical (C) | | APPD-08088 | Stablenet Prod | Critical (C) | | APPD-248492 | ToolsNet 8 W52.10 | Critical (C) | | APPD-03786 | VIRENSCHUTZ PROD | Critical (C) | | APPD-75396 | BMW SmartAutomationSuite | Uncritical (UC) | | APPD-13525 | EMC\_Prod | Uncritical (UC) | | APPD-180607 | Infrastructure Service PowerBI OnPremise PROD | Uncritical (UC) | | APPD-01312 | KM- Secureprint - Prod | Uncritical (UC) | | APPD-17138 | NSM Prod | Uncritical (UC) | | APPD-320376 | Symantec Protection Engine PROD | Uncritical (UC) | | APPD-91960 | Symantec\_Protection\_Engine\_Prod | Uncritical (UC) | | APPD-238938 | Sysmon Prod | Uncritical (UC) | | APPD-19882 | Trace Lab PROD | Uncritical (UC) | | APPD-308121 | Versiondog Plant 52 ;P52-prod | Uncritical (UC) | | APPD-13698 | Windows Server SCCM 2012 PROD | Uncritical (UC) | | APPD-17196 | XPegasus Platinum Body Shop;P52 PROD | Uncritical (UC) | | |

**Short description of scenario:**

A restoration of all damaged applications and network connectivity of Data Center/Network Room Building NCC1 (52.10/001.0/00.0/012) is required.

It is necessary to develop a project to improve the NCC2 structure to have space and power redundancy for server and storage replications that currently host only in NCC1.

Reference: Disaster Recovery Procedure - **3.2.3. Recovery procedures for Scenario Building NCC1 (52.10/001.0/00.0/012)**

Affected Business Processes are related:

* Body Shop Main Line and Finish Line
* Pre-Treatment/E-coat
* Sealer/UBS
* Paint Line
* Paint Finish
* Planning and Assembly of the Complete Body - F0-F1
* Testing and Finishing - F1-F2
* Assembly quality

#### Description of Scenario: Outage of room NCC2 - Araquari W52.10 (52.10/050.0/00.0/403)

|  |  |
| --- | --- |
| ***Scenario*** | ***Effects on IT Operations*** |
| Total unavailability of NCC2 (52.10/050.0/00.0/403) due to power outage. | Total network device outage on NCC2.  Limited functionality on the assembly line with no internet connectivity between Line 1 and Line 2.  No internet access in the assembly office area, including both LAN and WLAN.  Other buildings, such as the Paint Shop and Body Shop, remain unaffected by the room outage.  The backup system is currently inoperative, preventing the ability to perform local service backups or restore them due to server unavailability. |
| ***List of applications*** | |
| |  |  |  | | --- | --- | --- | | **Appl ID** | **Application** | **Criticality** | | APPD-12910 | Infrastructure Service NetBackup PROD | Critical (C) | | |

**Short description of scenario:**

Full network redundancy is essential, and possibly even an assembly building distribution that is separate from NCC2.

Reference: Disaster Recovery Procedure - **3.2.3. Recovery procedures for Scenario Building NCC2 (52.10/050.0/00.0/403)**

The only impact is the unavailability of the network in the Assembly office, in this case if people are move to another office the operation can continue running normally.

## Recovery Procedures

### Overview

Note: This is an overview plan on the activities of the single ITEE Task Force teams after they have been initiated by IT Crisis or IT Emergency Management Team to perform a Disaster Recovery. For more detailed Disaster Recovery Procedures please see the operation documentation (e.g. links in chapter 4) developed by the responsible global operations teams. Those procedures are generally valid for the respective technology.

**emergency teams**

(Global Operations Teams)

Status

**IT Crisis Management Team**IT Emergency Management Team

Critical Applications   
  
  
<https://apexpgma.bmwgroup.net/ords/f?p=567:80028:5928673480304>:::::

IT Infrastructure   
Components   
  
<https://cmdbp.bmwgroup.net/command/html/navigator/detail/zone/KYVX81P1BUQRRX>

Initialisation of Disaster Recovery Procedure

**DR Procedures**

Middleware   
Components

N/A

Check :  
Workplaces of IT emergency teams  
<https://atc.bmwgroup.net/confluence/display/ARAQUARIIT/Major+Incident+Management>

### Recovery Strategy

Brief description of IT Disaster Recovery Strategy for Araquari W52.10 / NCCs Outage

Servers and Storage hosted at NCC1 (52.10/001.0/00.0/012) are being backed up at NCC2 (52.10/050.0/00.0/403), but we don't have servers and storage replications, so it is not possible to perform an immediate failover of the NCC1 services to servers hosted on NCC2.

During any period when NCC1 is offline, access to applications hosted within that facility will be temporarily unavailable.

Both NCC1 and NCC2 have been equipped with redundancies for wired network, Wi-Fi network, and WAN circuit infrastructure. This redundancy ensures that, in the event of an outage in either facility, our manufacturing plant can maintain uninterrupted network services, safeguarding operational continuity.

In the event of a power failure in NCC1, as soon as power is restored to the installation, the recovery process will begin. This recovery is estimated to take approximately 1 hours

Similarly, in the event of power outages in NCC2, the recovery process will initiate once power returns to the facility. However, the recovery time in NCC2 is expected to be shorter, estimated at approximately 30 minutes.

After recovery, restrictions / limitations may be:

* reduced network performance;
* reduced network connectivity;
* limited access to applications hosted at NCC1 (52.10/001.0/00.0/012);

Operations "back to normal" is planned to be completed after 2 hours.

Consider implementing server and storage replications between NCC1 and NCC2. This will enable a seamless failover in the event of NCC1 outages, ensuring minimal disruptions to critical services.

### Recovery procedures for Scenario Room NCC1 - Araquari W52.10 (52.10/001.0/00.0/012)

The following Disaster Recovery approach for the specific scenario is adopted.

1. Call facilities management to engage electrical engineers.
2. Call Americas Infra-MIM to inform about the outage.
3. Turn on equipment as soon as power is restored.
4. Call central network operations to check and restore connectivity.
5. Call central server operations to check and restore servers.
6. Call central NAS operations team to check and restore servers.
7. Engage application operations and verify your application and test functionality.
8. Perform environment health checks.

The following characteristics must be taken into consideration when approaching disaster recovery for this environment.

1. Data center available? Yes
2. Data recovery center available? Yes
3. UPS available? Yes
4. UPS runtime [04h:00]
5. EPG available? No
6. EPG minimum runtime N/A

### Recovery procedures for Scenario Room NCC2 - Araquari W52.10 (52.10/050.0/00.0/403)

The following Disaster Recovery approach for the specific scenario is adopted.

1. Call facilities management to engage electrical engineers.
2. Call Americas Infra-MIM to inform about the outage.
3. Turn on equipment as soon as power is restored.
4. Call central network operations to check and restore connectivity.
5. Call central server operations to check and restore servers.
6. Call central NAS operations team to check and restore servers.
7. Engage application operations and verify your application and test functionality.
8. Perform environment health checks.

The following characteristics must be taken into consideration when approaching disaster recovery for this environment.

1. Data center available? Yes
2. Data recovery center available? Yes
3. UPS available? No
4. UPS runtime N/A
5. EPG available? No
6. EPG minimum runtime N/A

# Attachments

## IT Resources

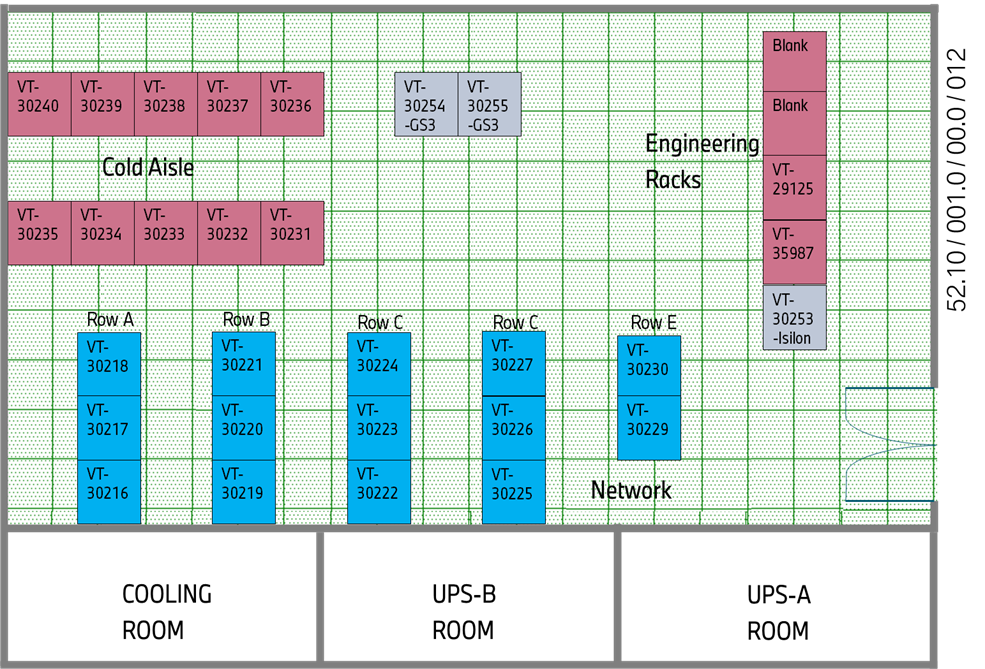


## List of abbreviations

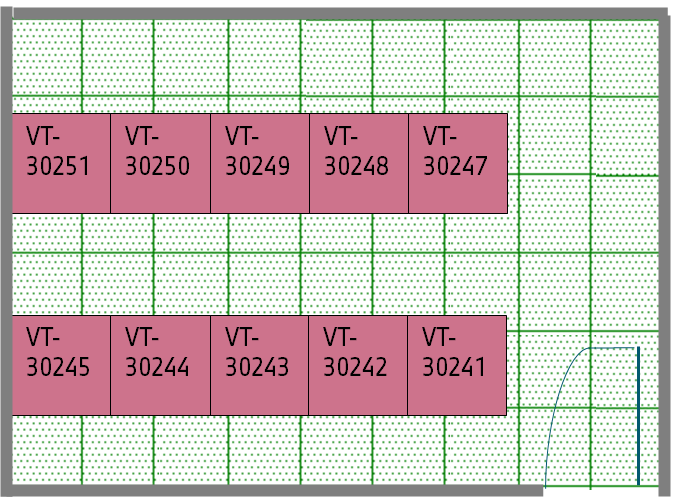
|  |  |
| --- | --- |
| BKO | Betriebliche Katastrophenschutzorganisation (translates to: Operational Catastrophe Protection Organisation) |
| MIM | Major Incident Manager |
| MOD | Manager on Duty |
| CMDB | Configuration Management Database |
| DC | Data Centre |
| DR | Disaster Recovery |
| ECM | Emergency Contact Management (system) |
| FACT24 | Automated alarming system |
| GSC | Group Security Center |
| CMDB | Configuration ManagementDatabase |
| TCM | Technical Continuity Management |
| LRE/IRE/OE | IT Service Continuity Manager per Area |
| USC | User Service Center |

## Layouts

### Data Center in building 52.10/001.0/00.0/012



### Data Center in building 52.10/050.0/00.0/403



# TEMPLATE Steering Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **BMW Group** | **Document class**: temporary | | | **Doc.-No.:** ITSCM-DOC-ID\_10 | |
| **Range of validity**: BMW Group | | | **Version**: 4 | |
| **IT Emergency Handbook Template** | | | **Status**:  Released, effective from 17th February 2020 | |
|  | **Coordinated with (person, dept, circle):** | | | Philipp Feldpausch, FG-8-I-1 | |
|  | | | | | |
| **Template Change history** | | | | | |
| **Version** | **Content of changes** | **Written by**  **Dept Code**  **Date** | **Reviewed by**  **Dept Code**  **Date** | | **Released by**  **Dept Code**  **Date** |
| 0.1 | Template IT Emergency Handbook (dev. Version 0.7) | IT-SCM Team,  FZ-401  14th July 2009 | IT-SCM Team,  FZ-401  14th July 2009 | | IT-SCM Team,  FZ-401  14th July 2009 |
| 0.11 | Update Template IT Emergency Handbook (dev. Version 0.71) | IT-SCM Team,  FZ-403  5th March 2010 | IT-SCM Team,  FZ-403  5th March 2010 | | IT-SCM Team,  FZ-403  5th March 2010 |
| 0.12 | Update Template IT Emergency Handbook Chapter 2.1.2. , 2.2.1. , 2.2.2. (dev. Version 0.72) | IT-SCM Team,  FZ-403  21st Nov. 2011 | IT-SCM Team,  FZ-403  21st Nov. 2011 | | IT-SCM Team,  FZ-403  21st Nov. 2011 |
| 0.13 | Update Template IT Emergency Handbook  (FZ -> FG), Chapter 1.7. (dev. Version 0.73) | IT-SCM Team,  FG-403  5th Nov. 2012 | IT-SCM Team,  FG-403  5th Nov. 2012 | | IT-SCM Team,  FG-403  5th Nov. 2012 |
| 0.14 | Update Template IT Emergency Handbook) misc. | ITSCM Team,  FG-903  18th Oct. 2013 | ITSCM Team,  FG-903  18th Oct. 2013 | | ITSCM Team,  FG-903  18th Oct. 2013 |
| 0.15 | Update Template IT Emergency Handbook) misc. | ITSCM Team,  FG-903  12th Jan.2015 | ITSCM Team,  FG-903  12th Jan.2015 | | ITSCM Team,  FG-903  12th Jan.2015 |
| 0-16 | Update  Document management information to cover page  Terminology updates: Critical to Major, CIM to MIM  Dept. codes updates: FZ-403, FG-403, FG-903 to FG-901 | Philipp Feldpausch,  FG-901  Mehran Majdi,  FG-91  9th Aug. 2016 | Philipp Feldpausch, FG-901  Mehran Majdi,  FG-91  9th Aug. 2016 | | Philipp Feldpausch, FG-901  Mehran Majdi,  FG-91  9th Aug. 2016 |
| 0-17 | Update chap. 2.1.1 about contact data of IT Info manager and IT Crisis Manager | Philipp Feldpausch, FG-901  2nd Feb.2017 | Philipp Feldpausch, FG-901  2nd Feb.2017 | | Philipp Feldpausch, FG-901  2nd Feb.2017 |
| 0.19 | Minor Changes | Philipp Feldpausch,  FG-813  9th Aug. 2016 | Philipp Feldpausch, FG-813  9th Aug. 2016 | | Philipp Feldpausch, FG-813  9th Aug. 2016 |
| 1 | Integration of template steering information (end of document) as well as document steering information (beginning of document) | Philipp Feldpausch, FG-813  9th July 2018 | Philipp Feldpausch, FG-813  9th July 2018 | | Philipp Feldpausch, FG-813  9th July 2018 |
| 2 | Update of link to IT Crisis Mgt. (itkm.bmwgroup.net is outdated, replaced by [*http://itcm.bmwgroup.net/*](http://itcm.bmwgroup.net/)*)* | Philipp Feldpausch, FG-813  6th August 2018 | Philipp Feldpausch, FG-813  6th August 2018 | | Philipp Feldpausch, FG-813  6th August 2018 |
| 3 | Chapter 1.3 deleted  Acceptance of the handbook moved to chapter 1.2  Dept. codes updated FG-901 replaced by FG-8-I-1 and replaced by ITSCM process owner  role TCM-A replaced by role LRE/IRE/OE  deleted TCM-A LT  and other minor changes | Philipp Feldpausch, FG-8-I-1  17th February 2020 | Philipp Feldpausch, FG-8-I-1  17th February 2020 | | Philipp Feldpausch, FG-8-I-1  17th February 2020 |
| 4. | Update throughout the document: Replaces ITSCM-A with LRE/IRE/OE  Page 4: Updated old email with [*ITSCM-Team@BMW.de*](mailto:ITSCM-Team@BMW.de)  Page 16: Updated Trigger and Disaster Scenarios.  Page 18, Par 3.1.2.1: Inserted Text and link to planning procedure. | Derik de Jager  FG-z-56  11 April 2022 | ITSCM Sub Product Team | | Christian Dreher  FG-8-I-3 |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |