Minutes of Meeting

LRE IT Management

Issued: 2026-02-06

Meeting: NIS 2 Update Meeting

Date: 2025-12-05

I. Personal Schulung und Überprüfungsprozesse > 1.1. Hintergrundcheck

#	Type	Description	Responsible	Due
1	Fact	1. Alle Besucher werden gegen die Sanktionsliste geprüft	-	-
2	Fact	2. Hintergrundscheck machen wir für Führungskräfte L1	-	-
3	Fact	3. Die Qualifikationsprüfung findet im Rahmen des Einstellungsgesprächs statt	-	-
4	Action	4. MB prüft mit HR (Adelina) ob ein Polizeiliches Führungszeugnis notwendig ist bzw. frequent nachgefordert werden sollte	Markus Bach	2026-01-30

I. Personal Schulung und Überprüfungsprozesse > 1.2. Schulung und Sensibilisierung

#	Type	Description	Responsible	Due
5	Fact	1. Mit der Einführung von Personio wird die Erfüllung der Trainings nachverfolgt	-	-
6	Fact	2. Die Cyber-Awareness-Schulung wurde in 2024 & 2025 durchgeführt	-	-
7	Action	3. Prüfen der Intranet-Präsenz und die Weiterentwicklung in Sharepoint è Caroline Kaufmann re. Marketing Präsenz	Markus Bach	2026-01-30

I. Personal Schulung und Überprüfungsprozesse > 1.3. Vertragliche Vereinbarung

#	Type	Description	Responsible	Due
8	Fact	1. Arbeitsverträge haben Sicherheitsanforderungen und Vertraulichkeitsvereinbarungen bzw. wurde aktualisiert	-	-
9	Action	2. MB prüft ob Vorfälle in dem Arbeitssicherheitsausschuss (ASA) registriert werden	Markus Bach	2026-01-30
10	Action	3. MB klärt, wie die Vorfälle HR-technisch registiert werden bzw. registriert werden können	Markus Bach	2026-01-30

I. Personal Schulung und Überprüfungsprozesse > 1.4. Sicherheit in der Lieferkette

#	Type	Description	Responsible	Due
11	Action	1. MB klärt mit dem Einkauf inwieweit derzeit Auskünfte z.b. D&B; erhoben und Verpflichtungen vertraglich nachgehalten werden	Markus Bach	2026-01-30

II. IT-Organisation and Cybersecurity > 1.1. Allgemeines

#	Type	Description	Responsible	Due
12	Fact	1. Prozesse wurden von S+P in Signavio dokumentiert	-	-
13	Action	2. Die Prozesse werden im Rahmen der ERP Neueinführung vertrieft und aktualisiert	Christian Kayser	2026-03-30

II. IT-Organisation and Cybersecurity > 1.2. IT-Organisation

#	Type	Description	Responsible	Due
14	Decision	1. Die Verantwortung für IT Sicherheit / BSI Kontakt wird an Simon Thorwart übertragen	Markus Bach	2025-12-05
15	Fact	2. Betriebsvereinbarung zur IT Richtlinie ist in Verhandlung mit dem Betriebsrat	-	-

II. IT-Organisation and Cybersecurity > 1.3. Zugriffskontrolle

#	Type	Description	Responsible	Due
16	Fact	1. Active Directory (AD) Projekt wird die Berechtigungen bereinigen	-	-
17	Fact	2. Single-Sign on wird bei Applikation in diesem Zuge forciert	-	-
18	Fact	3. MFA ist für die Office365, Bamboo und Teams umgesetzt	-	-

II. IT-Organisation and Cybersecurity > 1.4. Zutritt zu IT Räumen

#	Type	Description	Responsible	Due
19	Fact	1. Serverräume sind verschlossen (auch wenn Büro’s zugänglich sind)	-	-
20	Action	2. Stefan Rudolf wird die Zugangskontrolle zu den IT Büros einbauen – MB prüft den Fortschritt	Markus Bach	2026-01-30
21	Fact	3. Netzwerkschränke außerhalb des Serverraums	-	-
22	Fact	4. Netzwerksegmenierung führt das MacMon Tool ein und dieses führt bei Fremdgeräte zum Alarm und auch zur Sperre	-	-

II. IT-Organisation and Cybersecurity > 1.5. Mobiles Arbeiten

#	Type	Description	Responsible	Due
23	Action	1. Simon als IT Sicherheitsbeauftrage wird die Sicherheit beim mobilen Arbeiten prüfen und Empfehlungen formulieren	Simon Thorwart	-

II. IT-Organisation and Cybersecurity > 1.6. Cybersecurity

#	Type	Description	Responsible	Due
24	Fact	1. Cybersecurity Awareness Schulung in 2024 & 25 durchgeführt	-	-
25	Decision	2. Notfallhandbuch wird nach der Ernennung des NIS2 BIS Kontakt aktualisiert	Markus Bach	2025-12-05
26	Fact	3. ITA (Arbeitsanweisungen) werden derzeit überarbeitet und bis Q2 2026 aktualisiert sein	-	-
27	Action	4. PEN-Test wird für 2026 bis Mai eingeplant	Markus Bach	2026-06-29

II. IT-Organisation and Cybersecurity > 1.7. Incident Response

#	Type	Description	Responsible	Due
28	Fact	1. Incident Management System ist eingeführt	-	-

II. IT-Organisation and Cybersecurity > 1.8. Procuring Prozesse

#	Type	Description	Responsible	Due
29	Fact	1. Keine Ergänzungen notwendig	-	-

II. IT-Organisation and Cybersecurity > 1.9. Netzwerke

#	Type	Description	Responsible	Due
30	Fact	1. Netzwerksegmentierung am laufen und wird bis Mitte 2026 abgeschlossen sein	-	-
31	Fact	2. Netwerkmonitoring (PRTG) implementiert und wird stetig wo möglich auf Geräte ausgerollt.	-	-

III. Risikomanagement und BCM > 1.1. Business Continuity (IT Fokus)

#	Type	Description	Responsible	Due
32	Fact	1. Wiederanlaufpläne für Nördlingen aktualisiert und getestet	-	-
33	Fact	2. Wiederanlaufplan für München wird nach Serverneuaufbau aktualisiert und dann getestet	-	-
34	Fact	3. Redundante Server-, Netzwerk-, USV- und Backup-Architektur im Aufbau und bis Mitte 2026 fertig gestellt.	-	-
35	Fact	4. IFRI stellt einen Backup Server für das ERP System bis zu dessen Erneuerung	-	-

III. Risikomanagement und BCM > 1.2. Risikomanagement

#	Type	Description	Responsible	Due
36	Fact	1. Der Aufbau eines Risikomanagement Prozess auf Basis von den DocuSnap Daten ist für 2026 geplant	-	-
37	Fact	2. Die Hochrisikobereiche z.B. Netzwerk und ERP werden seit 2022 nach Priorität adressiert mit Ziel 2027 abzuschließen	-	-

IV. Betrieb und physische Sicherheit

#	Type	Description	Responsible	Due
38	Fact	1. Keine Ergänzungen notwendig	-	-

Generated: 2026-02-06 20:23 | Total entries: 38