

An
AIG Europe S.A, Direktion für Deutschland
zHd Herrn Torben Seyer, LL.M.
Brandstwiete 1
20457 Hamburg
Per Mail: torben.seyer@aig.com

Haus, am 28.12.2022

Sehr geehrter Herr Seyer,

vielen Dank für Ihre Nachricht. Im Zuge dieses Schreibens werden wir Ihnen folgend nach Rücksprache und unter zu Hilfenahme der KPMG, unseres IT-Dienstleisters ro² sowie unserer internen Ressourcen die von Ihnen angeforderten Informationen bereitstellen:

Welcher Zeitraum war für die Logretention des MAIL-SRVR zum Zeitpunkt des Incidents vorgesehen und konfiguriert? Wurden die Logs durch den Angreifer vernichtet oder waren diese aufgrund der tatsächlichen Logretention nur für den im KPMG Bericht genannten Zeitraum vorhanden.

Gemäß KPMG fallen für die konfigurierte Loggröße zu viele Logeinträge an, sodass diese nicht weit genug in die Vergangenheit zurückreichen. Dies sei für Server typisch. Es liegen jedoch keine Anzeichen dafür vor, dass der Angreifer die Logdateien gelöscht hätte.

Wann wurden welche Patches im letzten Jahr vor dem Angriff auf den MAIL-SRVR eingespielt? Innerhalb welchen Zeitraumes werden "neue" Patches jeweils eingespielt? Bitte übersenden Sie entsprechende Nachweise. Bitte teilen Sie uns in diesem Zusammenhang zudem mit, ob vorhandene kritische Exchange-Lücken der Server auf eine Kompromittierung untersucht wurden.

Patches für das Windows Betriebssystem und auch für den Exchange Server am MAIL-SRVR wurden regelmäßig sowie im Zuge anderer Wartungstätigkeiten installiert. Windows Updates wurde im Jahr 2022 installiert z.B. am 1./2.1.2022 (Exchange Jahr 2022-Problem) und 30.5.2022 (jeweils die letzten kumulativen Updates für Windows und .NET Framework). Mit der Wiederinbetriebnahme des Mailservers wurde das letzte verfügbare Exchange Server 2016 CU23 inkl. dem Security Update For Exchange Server 2016 CU23 (KB5019758) installiert. Alle Systeme unterliegen einem Wartungsplan, bei dem zumindest einmal binnen 2 Monate sämtliche verfügbaren Updates für Windows- und Microsoft-Server im Zuge eines geplanten Wartungsfensters installiert werden.

Aus Punkt 1.4 (Firewall Logs) des Bericht ergibt sich, dass ein externer Dienstleister für die Hauser Kaibling Seilbahn- und Liftges.m.b.H & Co. KG Logs tätig wird. Laut KPMG sei durch diesen die Herausgabe von älteren Logs verzögert bzw verhindert worden, „weshalb die Untersuchungen nach Rücksprache mit Hauser Kaibling am 05.12.2022 nicht durchgeführt wurden“. Hierzu bitten wir um Erläuterung.

Laut KPMG ist die Wahrscheinlichkeit auf Basis der Hostuntersuchungen als sehr gering eingestuft, über die Firewall-Logs noch werthaltige Informationen über den Angriff zu erlangen. Nach der Verzögerung der Übermittlung wurde gemeinsam beschlossen, dass die Analyse kosten/nutzentechnisch nicht sinnvoll ist. Dem Landeskriminalamt (LKA) stehen diese Logs jedoch für kriminalistische Untersuchungen zur Verfügung.

Lassen Sie uns bitte wissen, ob dem Landeskriminalamt – entsprechend der Empfehlung von KPMG – die Firewall Logs gemeinsam mit den anderen gesicherten Systemen zur Verfügung gestellt wurden.

Sämtliche kompromittierte Systeme sowie die Firewall Logs wurden gesichert und stehen diese dem LKA zum Download zur Verfügung. Bis dato kam es noch zu keinem Datentransfer. Dieser erfolgt nach gesonderter Aufforderung des LKA.

Bitte führen Sie aus, welchem Mitarbeiter der Benutzer „KnausAdm“ zugeordnet wurde. Unterlag dieser Account der Domain-Admin-Group? Falls ja: War dieser mit einer Multifaktor-Authentifizierung geschützt?

Der Benutzer KnausAdm war Mitglied der Domänen-Administratoren, was mit der Wiederinbetriebnahme des Domänencontrollers abgestellt wurde. Das Kennwort für dieses Konto konnte nicht ablaufen und es war nicht mittels MFA geschützt. Dieser User wurde für die Administration und Installationen von Applikationen verwendet.

Im vorliegenden Bericht wird von KPMG empfohlen, ein Security Assessment durchzuführen. Bitte lassen Sie uns wissen, ob Sie dieser Empfehlung folgen. Weiters bitten wir um Übermittlung der Ergebnisse des letzten Security Assessments.

Anlassbezogen wird ein Security Assessment im Nachlauf der Cyber Incident Behandlung unter Miteinbeziehung der Erkenntnisse erfolgen.

- In Ihrem Unternehmen etablierte Benutzer-Richtlinien zur Informationssicherheit bzw Datenschutzanweisungen

BB Hauser Kaibling



Stand Mai 2022 (ENTWURF)

IT-Sicherheitsrichtlinie

Inhalt

1	Versionsverlauf	4
2	Ziele.....	6
3	Geltungsbereich	6
4	Verantwortlichkeiten	7
5	Geheimhaltung.....	7
6	Richtlinien zum Umgang mit Daten & Geräten	7
6.1	Allgemein	7
6.2	Benutzerkonten.....	7
6.3	Passwörter.....	8
6.4	E-Mail	9
6.5	IT-Geräte & Smartphone	9
6.6	Umgang mit Wechseldatenträgern	10
6.7	Netzwerk	10
6.8	Anti-Virus.....	10
6.9	Entsorgung	10
6.10	Blogging & Social-Media.....	10
7	Alarmierung & Meldepflicht	11
8	Konsequenzen bei Verstößen	11
9	Auditierung & Sicherheitsüberprüfungen	11

Versionsverlauf

Version	Datum	Name / Rolle	Anmerkung
0.1	12.08.2021	Alfred Haas	Entwurf, 1.gültige Fassung
1.0	16.05.2022	Alfred Haas	2. gültige Fassung

Ziele

Das Ziel dieser Richtlinie ist die Definition von akzeptablem und nicht akzeptablem Umgang mit elektronischen Geräten, Netzwerkzugängen und Daten, unabhängig davon ob diese in digitaler oder schriftlicher Form existieren. Diese Richtlinie ist ergänzend zu ethischen und rechtlichen Rahmenbedingungen gültig.

Die [Firma] stellt Desktop-Computer, Notebooks, Smartphones und andere elektronische Systeme zur Verfügung, um die Unternehmensziele verfolgen zu können. Gleichzeitig ist das Unternehmen verpflichtet diese in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität zu schützen. Diese Richtlinie beinhaltet Maßnahmen, die ein jeder Mitarbeiter und jede Mitarbeiterin des Unternehmens einzuhalten haben, um das Unternehmen vor rechtlichen und finanziellen Schäden sowie einem Vertrauensverlust gegenüber Kunden zu schützen.

Geltungsbereich

Gültig für:

Hauser Kaibling Seilbahn- und Lift-Ges.m.b.H & Co KG
Erzherzog Johann Str. 180
8967 Haus

Und

Hauser Kaibling Betriebsges.m.b.H & Co KG
Erzherzog Johann Str. 180
8967 Haus

Beides i.F. zusammengefasst als Hauser Kaibling Seilbahn.

Alle MitarbeiterInnen der [Firma] haben sich konform zu dieser Richtlinie zu verhalten.

Diese Richtlinie gilt für alle Informationen und elektronischen Geräte, die den Mitarbeitern dauerhaft oder temporär zur Verfügung gestellt werden sowie für den Netzwerkzugang, der im Rahmen der beruflichen Tätigkeit verfügbar ist.

Verantwortlichkeiten

Für die Einhaltung, Messung und Verbesserung der Informationssicherheitsmaßnahmen sind der/die DatenschutzkoordinatorIn und die Abteilungsleiter zuständig.

Bei Fragen, Probleme, Sicherheitsvorfällen oder Verdachtsmomenten wenden Sie sich an den IT-Verantwortlichen.

Geheimhaltung

Im Rahmen Ihrer Tätigkeiten wird Ihnen Zugang zum Netzwerk des Unternehmens sowie zu Betriebsgeheimnissen, urheberrechtlich geschützten und anderen vertraulichen Dokumenten gewährt.

Sie verpflichten sich, diese Unterlagen und Informationen, auch über Ihr Dienstverhältnis hinaus, geheim zu behalten. Darüber hinaus gelten natürlich bereits vorhandene Geheimhaltungserklärungen die mit dem Dienstgeber unterzeichnet wurden.

Richtlinien zum Umgang mit Daten & Geräten

Allgemein

Sie sind zum verantwortungsvollen Umgang mit den Geräten und Daten der [Firma] nach bestem Wissen und Gewissen und unter Einhaltung der Richtlinien sowie rechtlicher Rahmenbedingungen verantwortlich. Geräte und Daten der [Firma] dürfen nicht für illegale oder verbotene Tätigkeiten verwendet werden.

Die bereitgestellten IT-Geräte und das Netzwerk sind ausschließlich für betriebliche Zwecke zu nutzen. Die Nutzung für private Zwecke ist untersagt. Die Nutzung von privaten Geräten im Netzwerk des Unternehmens ist ebenso untersagt.

Die Beschaffung und Installation von IT-Geräten erfolgt ausschließlich über die zentrale IT-Abteilung. Ein selbstständiges Herunterladen und Installieren von Anwendungen aus dem Internet ist untersagt.

Benutzerkonten

Der Zugang zum Unternehmensnetzwerk und betrieblicher Informationen wird Ihnen über die Bereitstellung eines personalisierten Benutzerkontos gewährt. Dieser Zugang ist auf Ihre Tätigkeiten abgestimmt und erhält die benötigten relevanten Zugriffsberechtigungen.

Die Zugangsdaten Ihres Kontos sind daher zu jedem Zeitpunkt geheim zu halten und dürfen nicht an andere, auch nicht an Kollegen, Vorgesetzte oder die IT-Abteilung, weitergegeben werden.

Passwörter

Ihr persönliches Benutzerkonto ist mit einem sicheren Passwort zu schützen. Ein sicheres Passwort besteht zumindest aus 10 zufällig kombinierten Zeichen der folgenden Zeichensätze:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

Darüber hinaus sollen keine vollständigen Wörter kombiniert mit Zahlen oder Sonderzeichen verwendet (z.B.: Helene!74) werden.

Das Passwort ist einmal pro Quartal zu wechseln.

Passwörter dürfen nicht auf Post-ITs, Word-, Excel- oder anderen unsicheren Dateiformaten bzw. Notizzetteln aufbewahrt werden. Passwörter sind zu merken oder alternativ in einem Passwort-Safe (<https://keepass.info/>) aufzubewahren. Benötigen Sie einen Passwort-Safe, können Sie diesen in der IT anfordern.

Aber auch bei der Verwendung anderer, nicht im betrieblichen Netzwerk befindlichen Anwendungen (z.B.: Projektmanagementplattformen, Ausschreibungsplattformen, usw.) sind sichere Passwörter zu verwenden. Darüber hinaus sollten bei verschiedenen Zugängen/Logins unterschiedliche Passwörter verwendet werden.

Anmeldungen auf maschinenbezogene PC's erfolgt mit Auto-Logon.

E-Mail

Die Nutzung des E-Mail-Postfaches der [Firma] ist ausschließlich für betriebliche Zwecke zugelassen. Der Versand von Spam-E-Mails oder Schadsoftware ist untersagt.

Eingehende E-Mails sind zudem auf Anzeichen von Phishing-E-Mails zu prüfen, insbesondere bevor eventuell inkludierte Anhänge oder Links geöffnet bzw. geklickt werden. Werden Sie im Zuge des Empfangs eines E-Mails von Ihrem Anti-Virus-Programm benachrichtigt, so löschen Sie die E-Mail.

Im Zweifelsfall wenden Sie sich an die IT-Abteilung.

IT-Geräte & Smartphone

Die Ihnen zur Verfügung gestellten IT-Geräte sowie das Smartphone sind Eigentum der [Firma]. Die bereitgestellten Geräte sind daher mit höchster Sorgfalt vor Verlust, Diebstahl und Zerstörung zu behandeln. Sollte einer dieser Fälle eintreten ist unverzüglich die IT-Abteilung zu benachrichtigen.

Bei Verlassen des Arbeitsplatzes ist sicherzustellen, dass Ihre Gerätschaften (PCs, Laptops, Smartphones) gegen Fremdzugriff gesperrt sind (Stichwort Bildschirmsperre/PIN).

Bei Reisen oder in der Öffentlichkeit sind die Geräte daher zu keinem Zeitpunkt ohne Aufsicht zurückzulassen. Bitten Sie zudem keine fremden Personen zur Aufsicht über Ihre Geräte.

Smartphones:

- dürfen auch privat genutzt werden
- Apps dürfen nur aus vertrauenswürdigen App-Shops (App-Store, Google-Play,...) installiert werden. Sollte man sich unsicher sein, kann man sich bei der IT-Abteilung erkundigen.
- Verbindung mit öffentlichen WLAN's nur für die Dauer der tatsächlichen Nutzung (z.B. Abruf Emails) aktivieren, danach wieder deaktivieren.

Umgang mit Wechseldatenträgern

Im Umgang mit IT-Geräten im Firmeneigentum dürfen auch nur Wechseldatenträger, welche Sie vom Unternehmen zur Verfügung gestellt bekommen haben, verwendet werden. Zur Vermeidung der Infizierung von Unternehmenseigentum mit schadhafter Software, dürfen diese Gerätschaften auch ausschließlich zu beruflichen Zwecken im Unternehmen verwendet werden.

Netzwerk

Der Zugriff zum Unternehmensnetzwerk ist ausschließlich für berufliche Zwecke zugelassen und über vom Unternehmen bereitgestellte Geräte gestattet. Ein Versuch die vorhandenen Sicherheitsmaßnahmen und den Zugriffsschutz zu umgehen, das Unternehmensnetzwerk aktiv anzugreifen oder eine absichtliche Störung herbeizuführen wird disziplinarisch geahndet.

Webseiten, die bekannterweise Schadsoftware, pornographische oder illegale Inhalte zeigen dürfen nicht aufgesucht werden. Das inkludiert größere oder illegale Downloads von Software, Videos, Bilder, Musik und anderem urheberrechtlich geschützten Daten.

Anti-Virus

Alle Geräte der [Firma] verfügen über einen aktuellen Anti-Virus Schutz, welcher die Systeme vor einer Infektion mit Schadsoftware schützen soll. Dieser ist daher keinesfalls zu deaktivieren oder anderweitig zu manipulieren.

Entsorgung

IT-Geräte beinhalten immer Betriebsgeheimnisse und andere vertrauliche Informationen. Die Entsorgung muss daher sicher durchgeführt werden und eine Wiederherstellung von Daten muss ausgeschlossen werden. Eine Entsorgung darf daher ausschließlich über die IT erfolgen.

Ist Ihr Gerät defekt oder muss dieses aus anderen Gründen getauscht werden, ist dieses immer an die IT zu retournieren.

Auch gedruckte und geschriebene Informationen beinhalten vertrauliche Informationen und sind sicher zu entsorgen. Entsorgen Sie sensible Dokumente daher immer nur über die bereitgestellten Shredder oder die verplombten Container.

Blogging & Social-Media

Die Nutzung von Blogs und sozialen Netzwerken während der Arbeitszeit ist grundsätzlich gestattet. Achten Sie aber auf eine faire und angemessene Nutzung und stellen Sie sicher, dass Ihre Arbeit durch die private Nutzung nicht beeinträchtigt wird.

Verzichten Sie bei der Verwendung von Blogs und sozialen Netzwerken auf Kommentare zu sensiblen Themen (z.B.: politische Meinungen, Hetze, religiöse Debatten, usw.) und veröffentlichen Sie keine rassenfeindlichen oder illegalen Bemerkungen.

Die [Firma] behält sich vor das Recht zur Nutzung von sozialen Netzwerken und Blogs jederzeit – auch in Einzelfällen – zu widerrufen.

Alarmierung & Meldepflicht

Aus der Europäischen Datenschutzgrundverordnung ergibt sich eine Meldepflicht bei der Verletzung des Schutzes von personenbezogenen Daten. Innerhalb von 72 Stunden ist die Datenschutzbehörde über eine solche Verletzung in Kenntnis zu setzen.

Dieses Zeitfenster kann nur durch die automatisierte Kontrolle der IT-Systeme sowie die Mitarbeit eines jeden einzelnen Mitarbeiters im Unternehmen eingehalten werden. Erkennen Sie Sicherheitsvorfälle oder haben Verdachtsfällen, so informieren Sie bitte umgehend den Datenschutzkoordinator oder den Abteilungsleiter. Dieser leitet die weiteren Schritte ein.

Konsequenzen bei Verstößen

Verstöße von MitarbeiterInnen gegen diese Richtlinien können disziplinarische Maßnahmen bis hin zur Kündigung nach sich ziehen. Verstöße von temporären Angestellten und Vertragspartnern können bis zur Terminierung des Vertragsverhältnisses führen.

Geräte, die zu einer Beeinträchtigung von anderen Geräten oder Nutzern führen, werden ohne Rücksprache vom Netzwerk getrennt.

Diese Richtlinie wurde nach bestem Wissen und Gewissen in Anlehnung an bestehende rechtliche Rahmenbedingungen und Gesetze erstellt. Widersprechen einzelne Passagen aktuell gültigen Gesetzen, so sind für diese Punkte, die gesetzlichen Rahmenbedingungen gültig und einzuhalten. Die restlichen Punkte dieser Richtlinie sind weiterhin gültig.

Auditierung & Sicherheitsüberprüfungen

Zum Schutz der Daten und Geräte der [Firma], sowie zum Zwecke der Wartung, ist es autorisiertem Personal ohne Vorankündigung möglich, die Geräte und den Netzwerkverkehr im Unternehmen nach Anomalien zu untersuchen sowie Sicherheitsüberprüfungen des Unternehmens, dessen Netzwerkes und einzelner Geräte durchzuführen.

- Nachweise, woraus sich ergibt, dass sämtliche Mitarbeiter der Hauser Kaibling Seilbahn- und Liftges.m.b.H & Co. KG mindestens jährlich IT-Sicherheits- und Datenschutzschulungen unterzogen werden.

Sämtliche relevante Mitarbeiter werden gemäß Organisationshandbuch im Prozess Onboarding ua in die IT-Sicherheitsrichtlinie unterwiesen.

Onboarding

Grundsatz

Die Kurzform Onboarding stammt ursprünglich aus dem Amerikanischen und steht für „taking on board“ – grob übersetzt: „neue Mitarbeiter an Bord holen“. Gemeint ist die systematische Integration und Einarbeitung neuer Mitarbeiter im Unternehmen. Ziel ist, den Neuzugang fachlich einzuarbeiten und zügig ins Team und in die Unternehmenskultur einzugliedern.

3 Phasen Modell:

1. Phase: Preboarding
2. Phase: 1.Arbeitstag
3. Phase: In der Probezeit

1. Phase PREBOARDING <i>Administration mit Bereichsleitung</i>	Vorbereitende Tätigkeiten für den Arbeitsantritt: Ankündigung im Betrieb (per Mail, mit Namen, Position, Arbeitsbeginn,...) Arbeitsplatz festlegen/einrichten (falls benötigt Technik miteinbeziehen) Daten des MA (Familienstand, Sozialversicherungsnummer, Bankverbindung, ...) Anmeldung des MA (unbedingt vor Arbeitsbeginn) Vertrag vorbereiten – Infos dazu (Wochenstunden, Lohn) von BL einholen Arbeitsunterlagen/Betriebsinformationen vorbereiten – Infomappe Info Hauser Kaibling Info Organisationshandbuch – Version über Verantwortungsbereiche Kopien Dienstvertrag und Anlagen Telefonliste Je nach Bereich Schlüssel/Schlüsselkarte und Alarmchip vorbereiten Telefon/Handy mit DW Chip für Zeiterfassung vorbereiten	
--	---	--

	Computer und Mail Adresse anlegen Genauer Vereinbarung von Lohn und Wochenstunden Direkte Kollegen informieren (evtl. Ansprechperson bestimmen) Arbeitskleidung vorbereiten	
2. Phase 1.ARBEITSTAG <i>Bereichsleitung</i>	Der erste Arbeitstag hinterlässt sehr viele Ersteindrücke und muss sich dafür von den Bereichsleitern Zeit genommen werden. Begrüßung des neuen MA Arbeitsplatz zeigen Infomappe übergeben und Erläuterung Rundgang im Gebäude/Arbeitsbereich Vorstellung bei den anderen BL´s und direkten MA Erläuterung IT-Sicherheitsrichtlinie und Unterweisung durch BL und Verantwortlicher In Aufgaben einweisen	
3. Phase PROBEZEIT <i>Bereichsleitung</i>	Evaluierung des Dienstnehmers und Feedback im BL-Meeting Mitarbeitergespräche führen Funktionieren alle Geräte und Zugänge? Weiterbildung – gibt es Schulungen die der MA machen sollte/möchte? Sind alle Aufgaben klar? Wie kommt der neue MA zurecht?	

Des Weiteren werden gemäß 11 Information und Kommunikationsstrukturen im Zuge der BL Meetings die oben angeführte IT-Sicherheitsrichtlinie erläutert.

Information und Kommunikationsstrukturen

Grundsatz zur Informationsversorgung

Der/die jeweilige Verantwortliche/r für eine Aufgabe ist auch dafür verantwortlich, dass die relevanten Informationen zeitnah und vollständig an die relevanten Personen weitergegeben werden („Bringschuld“)!
Bei besonderen Situationen ist die Information und Kommunikation in der BL-Runde abzustimmen und zu vereinbaren

Störungen:

Zuständiger Betriebsleiter meldet Stillstand sofort an den Infopoint per Telefon (allgemeine Officenummer 3030)

Infopoint verteilt Information an Office & Finanzen, Kassa bzw. Marketing

Marketing aktualisiert Laufschriften der Panoramatafeln

Generelle Regelungen für Kommunikationsstrukturen

Schriftliche Einladung mit Themen bzw. Tagesordnung – gilt für Betriebsbesprechung und Sitzungen in großen Zeitabständen

Sitzungsleitung und Protokollführung durch Verantwortlichen

Protokoll: Sitzungsprotokoll inkl. Aktivitätenplan (**WAS, WER, bis WANN**) → siehe Musterprotokoll

Bezeichnung	TeilnehmerInnen	Verantwortlich Durchführung	Zweck/Inhalt	Intervall/Häufigkeit
Bereichsleiterbesprechung	- GF, BL - Beschneidung, Office & Finanzen, Marketing, Betriebsrat	GF, Office & Finanzen	- Informationsaustausch, operatives Geschäft - Projekte	14-tägig Dienstag 11:30 Uhr (max. 1,5h)
Office & Finanzen Jour fixe	GF, Office & Finanzen	GF, Admin	Abstimmung mit GF zu Office & Finanzen	14-tägig Dienstag, 07:45 Uhr
Marketing Jour fixe	GF, Marketing	GF, Marketing	Abstimmung mit GF zu Marketingaktivitäten	14-tägig Dienstag, 08:30 Uhr

			Information über aktuelle Themen	
Piste/Beschneigung - JF	BL, GF	GF, Piste/Beschneigung	Abstimmung Piste/Beschneigung mit GF	14-tägig Dienstag, 10:00 Uhr
Betrieb Jour fixe	BL, GF	GF, Betrieb	Abstimmung GF mit Betrieb	14-tägig Dienstag, 10:45 Uhr
IT-Security	BL	Bahnen&Technik	Adaption/Erläuterung IT-Sicherheit und Datenschutz im Zuge BL Meeting	1 Mal p.a.
Kassa-besprechung	Admin, Kassa inkl. Höfi und Sampl, Infopoint	Office & Finanzen	Informationsweitergabe über Neuerungen (in Absprache mit Marketing)	4 Mal p.a. Saisonbeginn und Saisonende (Sommer und Winter)
Betriebsschulung	Seilbahnmitarbeiter	BL	- Schulung durch BL - Unterweisung durch Sicherheitsfachkraft	2 Mal p.a. Saisonbeginn
Parkplatzmitarbeiter Schulung	Parkplatzmitarbeiter, BL	BL	- Schulung durch BL - Unterweisung durch Sicherheitsfachkraft	1 Mal p.a. Vor Wintersaison
Maschinenbesprechung	Alle Maschinisten und Betriebsleiter	BL	- Informations- und Erfahrungsaustausch - Ideen, Vorschläge	2 Mal p.a. Saisonbeginn
Skigebietsbefahrung	Bereichsleiter	GF, Marketing	- Informations- und Erfahrungsaustausch - Ideen, Vorschläge - Saisonauswertung und Handlungsfelder definieren	1 Mal p.a. Wintersaison

Saisonabschlussfeier / Weihnachtsfeier	• Alle	Marketing, Office & Finanzen		1 Mal p.a.
---	--------	------------------------------	--	------------

BL Meetings

Jour fixe Piste

Jour fixe Bahnen

Jour fixe Office

Jour fixe Marketing

Jour fixe Bahnen u Technik

Aktenvermerk

Seite hinzufügen

BL-Meeting 07.09.2021

BL Meeting 15.09.2021

BL Meeting 11.10.2021

BL Meeting 19.10.2021

BL Meeting 16.11.2021

BL Meeting Betriebstag 1

BL Meeting 06.12.2021

BL Meeting 14.12.2021

BL Meeting 10.12.2021

BL Meeting 23.12.2021

Meeting 30.12.2021 COVID

BL Meeting 07.01.2022

BL Meeting 28.01.2022

BL Meeting 08.02.2022

BL Meeting 22.02.2022

ICG Workshop Org-Handbuch

BL-Meeting 08.03.2022

BL Meeting 22.03.2022

Betriebsbesichtigung Kitzbühne

BL Meeting

BL Meeting 15.04.2022

Feedback Saison 21/22

BL Meeting 04.05

BL Meeting 17.05.2022

BL Meeting 14.06.2022

BL Meeting 28.06.2022

BL Meeting 12.07.2022

BL Meeting 09.08.2022

BL Meeting 23.08.2022

BL Meeting 08.09.2022

BL Meeting 20.09.2022

Seite ohne Titel

Seite ohne Titel

BL Meeting 11.10.2022

BL Meeting 17.05.2022

Dienstag, 17. Mai 2022 11:34

Anton, Michi, Thomas, Thomas R. Carina, Petra, Alfred, GF, Evi, Sabine, MH, Herbert, Mario

AGENDA:

IT-Sicherheitsrichtlinie Update

Dokument IT-Sicherheitsrichtlinie Version 1.0 - Dokument

Sommerbetrieb