Sicherheitsrichtlinie Microsoft Teams

TU Clausthal, Rechenzentrum

Version 1.8 - 03.09.2026

Dokumentinformationen

Version	Datum	Änderung	Autor
1.4	27.05.2025	Diverse Formulierungen	Martin Diedrich
1.5	04.07.2025	Kapitel 3, Ergänzung Schutzstufen-konzept LfD NDS	Martin Diedrich
1.6	09.09.2025	Ergänzungen hinzugefügt	Nils-Ruven Bähr
1.7	01.10.2025	Letzte redaktionelle Anpassungen	Martin Diedrich
1.8	03.09.2026	Hinweis zu Umfragen	Martin Diedrich

Inhaltsverzeichnis

Hinweis:
Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

1 Gkpnqgkvwpi

1.1 Zielsetzung

Diese Richtlinie definiert die Sicherheitsanforderungen an die Kollaborationslösung Microsoft Teams. Das Ziel ist eine angemessene und sichere Nutzung der Anwendung und der darin verarbeiteten und abgelegten Informationen.

Die konkreten Ziele dieser Richtlinie im Kontext der Informationssicherheit sind:

- Schutz der Vertraulichkeit: Gewährleistung, dass sensible Informationen, die in der Lösung ausgetauscht werden, vertraulich behandelt werden. Dies umfasst den Schutz vor unbefugtem Zugriff auf Daten und die Verhinderung von Lecks.
- Gewährleistung der Integrität: Sicherstellen, dass die in der Lösung gespeicherten oder übermittelten Daten korrekt und unverändert bleiben. Dies beinhaltet den Schutz vor unbefugten Änderungen oder Manipulationen.
- Verfügbarkeit sicherstellen: Sicherstellen, dass die Kollaborationslösung stets verfügbar ist, um die Kommunikation und Zusammenarbeit der Benutzer zu unterstützen. Dies umfasst Maßnahmen zur Vermeidung von Ausfallzeiten und zur Wiederherstellung nach Störungen.
- Schutz vor Malware und Bedrohungen: Implementierung von Mechanismen zur Erkennung und Abwehr von Malware, Phishing-Angriffen und anderen Sicherheitsbedrohungen.
- Benutzerbewusstsein und Schulung: Sensibilisierung der Benutzer für Sicherheitsrisiken und Bereitstellung von Schulungen zur sicheren Nutzung der Kollaborationslösung.
- Compliance mit gesetzlichen Anforderungen: Sicherstellen, dass die Lösung, mit den beeinflussbaren Möglichkeiten, den geltenden Datenschutz- und Sicherheitsvorschriften entspricht.
- Notfallplanung und Reaktion: Festlegung von Verfahren zur Bewältigung von Sicherheitsvorfällen, einschließlich Notfallwiederherstellung und Kommunikation mit Benutzern.

1.2 Geltungsbereich

Der Geltungsbereich umfasst alle Benutzer, Systeme, Daten und Aktivitäten, die an der TU Clausthal im Zusammenhang mit der Nutzung von Microsoft Teams stehen.

Konkretisiert sind das:

- Benutzer: Alle Mitarbeiter, Studierende, Auftragnehmer und Dritte, die autorisierten Zugang zu Microsoft Teams erhalten.
- Systeme: Alle Geräte die direkt oder indirekt mit der Kollaborationslösung verbunden sind.
- Daten: Jegliche Daten, Informationen oder Inhalte, die in Microsoft Teams erstellt, geteilt, gespeichert oder verarbeitet werden.
- Aktivitäten: Alle Aktivitäten, die im Rahmen der Nutzung von Microsoft Teams durchgeführt werden, einschließlich Kommunikation, Dateiaustausch, Zusammenarbeit an Dokumenten usw.

Verstöße können für Mitarbeiter zu arbeits-, disziplinar- und/oder strafrechtlichen Konsequenzen führen.

Abweichungen von dieser Richtlinie sind nur in begründeten Ausnahmefällen zulässig und vorher beim Informationssicherheitsbeauftragten (im Folgenden „ISB“ genannt) zu beantragen und von ihm zu genehmigen.

1.3 Rechtliche Anforderung

Diese Sicherheitsrichtlinie begründet sich damit, den Anforderungen der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) gerecht zu werden und die notwendige Sicherheit und Datenschutz für die verarbeiteten Daten zu gewährleisten.

Gemäß der DSGVO und des BDSG müssen Organisationen sicherstellen, dass personenbezogene Daten angemessen geschützt werden, um die Rechte und Freiheiten der betroffenen Personen zu wahren. Dies bedeutet, dass geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu gewährleisten.

Dazu gehört auch die Implementierung von Sicherheitsrichtlinien für Tools wie Microsoft Teams, die es den Benutzern ermöglichen, sicher und verantwortungsvoll mit personenbezogenen Daten umzugehen. Die Sicherheitsrichtlinie definiert klare Verfahren und Best Practices für die sichere Nutzung von Microsoft Teams, einschließlich der Konfiguration von Datenschutzeinstellungen, Zugriffskontrollen, Verschlüsselung und Maßnahmen zur Verhinderung von Datenlecks. Durch die Einhaltung dieser Richtlinie können Organisationen sicherstellen, dass die Datenschutzanforderungen eingehalten werden und die verarbeiteten Daten angemessen geschützt sind.

2 Xgtcpvy qtvrlkej mgkvgp

Indem klare Verantwortlichkeiten definiert werden, kann die Organisation sicherstellen, dass die Sicherheitsrichtlinien für Microsoft Teams effektiv umgesetzt und eingehalten werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen zu gewährleisten.

2.1 Systemadministratoren

Die Systemadministratoren sind verantwortlich für die Konfiguration, Überwachung der technischen Aspekte und Durchsetzung der Sicherheitsrichtlinien in Microsoft Teams. Dazu gehört das Festlegen von Berechtigungen, das Implementieren von Sicherheitsmaßnahmen und das Überwachen von Aktivitäten.

2.2 Benutzer

Die Benutzer sind verantwortlich für die Einhaltung der Sicherheitsrichtlinien während der Nutzung von Microsoft Teams. Dazu gehört die sichere Handhabung von Informationen, die Verwendung von sicheren Kennwörtern, die Meldung von Sicherheitsvorfällen und die Einhaltung der festgelegten Sicherheitsrichtlinien.

2.3 Informationssicherheitsbeauftragter (ISB)

Der ISB trägt die Verantwortung für die fortlaufende Bewertung und Aktualisierung der Sicherheitsrichtlinien für Microsoft Teams. Er ist dafür zuständig, Bedrohungen zu identifizieren, Sicherheitslücken zu schließen und sicherzustellen, dass die Richtlinien den aktuellen Best Practices entsprechen.

Zudem ist der ISB verantwortlich für die Sicherstellung, dass die Nutzung von Microsoft Teams im Einklang mit den geltenden rechtlichen Anforderungen und Unternehmensrichtlinien steht. Sie überwachen die Einhaltung von Vorschriften und stellen sicher, dass entsprechende Maßnahmen ergriffen werden, um die Einhaltung sicherzustellen.

2.4 Management und Führungsebene

Das Management und die Führungsebene tragen die Verantwortung dafür, die Bedeutung von Sicherheit in Microsoft Teams zu betonen und die notwendigen Ressourcen bereitzustellen, um sicherzustellen, dass die Sicherheitsrichtlinien wirksam umgesetzt werden können. Sie sind auch dafür verantwortlich, eine Sicherheitskultur innerhalb der Organisation zu fördern und die Bedeutung der Einhaltung von Sicherheitsrichtlinien zu kommunizieren (vgl. IT-Sicherheitsrichtlinie der TU Clausthal).

3 Ukej gtj gkvumqphkuwtcvkqp

Hier werden die empfohlenen Sicherheitseinstellungen für Microsoft Teams beschrieben, einschließlich der Konfiguration von Berechtigungen, Zugriffssteuerung und Datenschutzeinstellungen.

3.1 Zu verarbeitende Daten und Verschlüsselung

Es sind im Geltungsbereich dieser Richtlinie ausschließlich dienstliche Daten zu verarbeiten. Die Verarbeitung von bzw. Vermischung mit privaten Daten ist explizit ausgeschlossen.

In sämtlichen Kommunikationsbereichen in Microsoft Teams, sowohl im Chat, als auch in Meetings, als auch in dedizierten Teams oder Kanälen, dürfen keine Informationen mit einem erhöhten Schutzbedarf, wie beispielsweise personenbezogene Daten gemäß Artikel 9 der Datenschutz-Grundverordnung (DSGVO), abgelegt oder verarbeitet werden.

Informationen, die im Umkehrschluss über einen normalen Schutzbedarf hinausgehen, werden in dafür vorgesehenen Lösungen/Fachverfahren des Unternehmens verarbeitet und abgelegt. Das Schutzstufenkonzept des Landesbeauftragten für den Datenschutz Niedersachsen ist zu beachten - grundsätzlich sollen im M365/MS Teams nur Daten der Kategorien[1] A und B verarbeitet werden. Bei Daten der Kategorie C ist die Verarbeitung innerhalb eines bestehenden Fachverfahrens oder anderer, datensparsamerer Verarbeitungsmöglichkeiten „on Premise" vorzuziehen.

In der Konsequenz ist eine gesonderte Verschlüsselung neben den vom Hersteller durchgeführten Verschlüsselungsmechanismen nicht notwendig. Alle in Microsoft Teams verarbeiteten Daten werden durch den Hersteller sowohl bei der Übertragung als auch im Ruhezustand automatisch verschlüsselt. Eingesetzt werden hierbei die Protokolle TLS und SRTP.

3.2 Sichere Installation & Aktualisierung

Das zentrale Deployment des Rechenzentrums beinhaltet die aktuelle Version von MS Teams.

Sofern nicht vom RZ zentral bereitgestellte Rechner zum Einsatz kommen, ist die Installation von MS Teams eigenständig durchführbar.

Eine automatische Aktualisierung findet im Rahmen der Microsoft-Teams-Updates herstellerseitig statt.

3.3 Regelung zum Autostart

Mitarbeiter können in der Teams App unter "Allgemein – System – Teams automatisch starten" das Verhalten der Anwendung beeinflussen. Dadurch kann der Benutzer eigenständig entscheiden, wann er sich in Microsoft Teams einloggt und online geht. Dieser Ansatz gewährleistet eine bewusste und eigenverantwortliche Nutzung der Plattform

[1] Erläuterungen zu den Kategorien finden Sie im Anhang (5.) unter Datenschutz-Kategorien

durch die Benutzer, während gleichzeitig eine ungewollte Übermittlung von Statusinformationen vermieden wird.

3.4 Umgang mit Profilbild

Die Verwendung von Profilbildern geschieht auf freiwilliger Basis. Geben Mitarbeiter das Einverständnis zur Nutzung ihres Profilbildes, können sie dieses selbstständig in der Microsoft Teams App hochladen und nutzen bzw. dieses wieder entfernen.

3.5 Umgang mit Präsenzstatus

Standardmäßig können alle Benutzer innerhalb einer Organisation sehen, ob ein anderer Benutzer online verfügbar ist. Es gibt verschiedene verfügbare Präsenzstatus in Teams, darunter "Verfügbar", "Beschäftigt", "Nicht stören", "Bin gleich zurück", "Abwesend" und "Offline". Der Anwesenheitsstatus basiert auf Benutzeraktivitäten, Outlook-Kalenderstatus oder dem Status der Teams-App.

Der Status kann auch manuell gesetzt werden, wobei die Dauer der Einstellung definierbar ist.

3.6 Persönliche Einstellungen in Microsoft Teams App

Die persönlichen Einstellungen innerhalb der Microsoft Teams-App müssen durch jeden Benutzer manuell gesetzt werden. Die Grundeinstellungen werden wie folgt empfohlen:

- Microsoft Teams App - Einstellungen - Datenschutz
  - Mich in Anwesenheitsberichten identifizieren -> **deaktivieren**
  - Diagnosedaten anzeigen -> **deaktivieren**
  - Optionale verbundene Erfahrungen -> **deaktivieren**

- Microsoft Teams App - Einstellungen - Barrierefreiheit - Untertitel und Transkripte
  - Mich automatisch in Live-Untertiteln und Live-Transkripten identifizieren -> **deaktivieren**
  - Immer Untertitel in meinen Anrufen und Besprechungen anzeigen -> **deaktivieren**

Durch diese Konfiguration wird sichergestellt, dass persönliche Daten geschützt sind und keine unerwünschten Informationen über den Benutzer offengelegt werden. Es ermöglicht den Benutzern auch, ihre Präferenzen hinsichtlich der Anwesenheitsberichten und Diagnosedaten anzupassen, um ihre Privatsphäre zu wahren.

3.7 Microsoft Teams – Administrative Richtlinien

Zentral für alle Teams definierte Richtlinien:

Microsoft Teams – Teams – Teams Einstellungen, zulässig ist:
- Private Kanäle erstellen
- Freigegebene Kanäle erstellen
- Benutzer können E-Mails an eine Kanal-E-Mail-Adresse senden
- Wer Tags verwalten kann -> Team-Besitzer/-Mitglieder

- Team-Besitzer können festlegen, wer Tags verwalten kann

Microsoft Teams – Teams – Team Vorlagen
- Aktuell sind keine Teams Vorlagen definiert

Microsoft Teams – Nachrichten – Nachrichten
- Besitzer können gesendete Nachrichten löschen
- Gesendete Nachrichten löschen
- Chat löschen
- Gesendete Nachrichten bearbeiten
- Lesebestätigung -> zentral deaktiviert
- Chatten mit Gruppen
- Unangemessenen Inhalt melden
- Sicherheitsbedenken melden
- Dringende Nachrichten mit Prioritätsbenachrichtigungen senden
- Benutzer aus Gruppen-Chats entfernen
- Vorgeschlagene Antworten im Chat anzeigen -> zentral deaktiviert
- URL-Vorschauen

Microsoft Teams – Users – Gastzugriff
- Aktuell ist der Gastzugriff global deaktiviert

Microsoft Teams – Users – Externer Zugriff
- Alle externen Domänen werden blockiert (es wird keiner externen Domäne vertraut)

3.8 Microsoft Teams – Chat

Alle Chat-Kommunikation in MS Teams läuft über die Microsoft-Cloud.

Für eine sichere und datenschutzkonforme Nutzung des Chats in Microsoft Teams sind folgende Maßnahmen zu beachtet:

- Wissen Sie immer, wer Mitglied im aktuellen Chat ist.

- Übertragen Sie keine sensiblen oder vertraulicher Informationen über den Chat.

- Seien Sie vorsichtig, wenn Sie Links, Dateien oder Anhänge über den Chat erhalten. Es ist entscheidend, verdächtige Inhalte nicht zu öffnen oder auf verdächtige Links nicht zu klicken. Dies betrifft sowohl interne, vor allem aber auch externe Kommunikationspartner.

3.9 Microsoft Teams – Meetings

Der Organisator eines Microsoft Teams-Meetings hat verschiedene Aufgaben und Verantwortlichkeiten.

3.9.1 Organisation/Einladen zu Meetings

Der Organisator plant Meetings, einschließlich der Festlegung von Datum, Uhrzeit und Dauer sowie der Teilnehmer. Es ist wichtig sicherzustellen, dass nur die Personen eingeladen werden, die für das Meeting relevant sind, und die Zugang zu den im Meeting vorhandenen Informationen haben dürfen. Der Organisator verwaltet auch die Teilnehmerliste, überwacht Anmeldungen und Absagen und aktualisiert Informationen für die Teilnehmer.

Während des Meetings übernimmt der Organisator die Moderation der Diskussion und stellt sicher, dass Änderungen wie das Verlassen von Teilnehmern oder das Hinzufügen weiterer Personen kommuniziert und kenntlich gemacht werden. Durch diese Maßnahmen trägt der Organisator dazu bei, dass das Meeting reibungslos abläuft und die Ziele erreicht werden.

3.9.2 Ausblenden des Hintergrunds bei Videokonferenzen

Microsoft Teams bietet die Möglichkeit, den Hintergrund von Videokonferenzübertragungen zu verschleiern, sodass nur das Bild des Sprechers übertragen wird. Diese Funktion sollte eingesetzt werden, um einen versehentlichen Abfluss von Informationen oder eine Erfassung von Bildern unbeteiligter Personen zu vermeiden.

Durch die Verwendung dieser Funktion wird die Privatsphäre der Benutzer geschützt und das Risiko ungewollter Offenlegungen von sensiblen Informationen reduziert.

3.9.3 Start eines Meetings

Zu Beginn muss eine Überprüfung der Meeting-Einstellungen durch den Meeting-Owner erfolgen. Während der folgenden Einwahl der Teilnehmer folgt dann die wichtige Prüfung der Identitäten - vor allem bei Teilnehmern, die sich telefonisch einwählen. Hier sollte die Identität z.B. anhand der Stimme oder gezielter Fragen validiert werden.

Es sollte immer ein virtueller Warteraum genutzt werden, um die Identität der Teilnehmer zu überprüfen, insbesondere bei der reinen Audio-Einwahl. Virtuelle Warteräume schützen vor unbefugtem Zugriff und unbemerkter Anwesenheit von Teilnehmern.

Teilnehmer werden automatisch angezeigt, und der Organisator ist dafür verantwortlich sicherzustellen, dass der Eintritt und Austritt von Teilnehmern allen anderen in der Konferenz signalisiert wird.

3.9.4 Weitere Teilnehmer hinzufügen

Wie bereits unter „Start eines Meetings“ beschrieben, ist der Meeting-Organisator dafür verantwortlich sicherzustellen, dass der Eintritt und Austritt von Teilnehmern allen anderen in der Konferenz signalisiert wird.

3.9.5 Aufnahme von Konferenzinhalten

Die Aufzeichnung von Konferenzen ist nur in Ausnahmefällen vorgesehen und wird auf Anfrage freigeschaltet. Der Nutzungszweck solcher Aufzeichnungen muss den Meeting-Teilnehmern im Vorfeld bekannt gegeben, nachvollziehbar eine Zustimmung eingeholt werden und diese dauerhaft dokumentiert werden. Eine technische Abfrage der Zustimmung muss daher in den Besprechungsoptionen eingestellt werden. Sofern kein Einverständnis gegeben wurde, werden diese Teilnehmer stummgeschaltet und die Kamera deaktiviert.

Nach Beendigung der Aufnahme wird der Inhalt im Meeting unter „Dateien“ abgelegt. Jeder Meeting-Teilnehmer hat automatisch Zugriff auf diesen aufgenommenen Inhalt, kann ihn jedoch nicht verändern. Um einen Zugriff auf diese Aufnahme zu unterbinden, müssen die jeweiligen Teilnehmer vom Meeting-Organisator aus dem Meeting entfernt werden. Benötigen weitere Mitarbeiter Zugriff auf die Inhalte, müssen diese dem Meeting im Nachgang hinzugefügt werden.

3.9.6 Auswertungen von Konferenzinhalten

Soll eine Konferenz aufgezeichnet und hieraus die Konferenzinhalte ausgewertet werden, muss neben dem Einverständnis zur Aufnahme gesondert und nachvollziehbar eine Zustimmung der teilnehmenden Parteien eingeholt und diese dauerhaft dokumentiert werden.

Für Auswertungen während einer Konferenz muss der Meeting-Organisator sicherstellen, dass nur solche Auswertungen möglich sind, die den Richtlinien der Institution und der geltenden Gesetzeslage entsprechen. Eine Auswertung und Analyse von Verhalten von Teilnehmern oder deren emotionaler Zustände sind nicht gestattet.

3.9.7 Dateiablage

Stellen Sie sicher, dass nur autorisierte Benutzer Teilnehmer des Meetings sind, welche Zugriff auf die Dateien haben dürfen.

Vermeiden Sie das Speichern/Ablegen sensibler oder vertraulicher Informationen über die Dateiablage innerhalb des Meetings, es sei denn, dies ist unbedingt erforderlich. Informationen mit einem erhöhten Schutzbedarf, wie beispielsweise personenbezogene Daten gemäß Artikel 9 der Datenschutz-Grundverordnung (DSGVO), dürfen nicht abgelegt oder verarbeitet werden.

3.9.8 Bildschirmübertragung

Beim Teilen des Bildschirms in Microsoft Teams müssen verschiedene Sicherheits- und Datenschutzaspekte beachtet werden:

Jeder Mitarbeiter muss sicherstellen, dass keine sensiblen oder vertraulichen Informationen auf dem Bildschirm angezeigt werden, während Sie den Bildschirm teilen. Dies gilt insbesondere für personenbezogene Daten, geistiges Eigentum, vertrauliche Geschäftsinformationen oder andere sensible Daten. Entfernen Sie auch z.B. Dateien mit Bewerbernamen von Ihrem Desktop. Denken Sie an Bilder mit Thumbnails auf dem Desktop oder in der Explorer-Ansicht.

Teilen von Anwendungen statt des gesamten Bildschirms: Teilen Sie grundsätzlich nur bestimmte Anwendungen oder Fenster auf Ihrem Bildschirm anstatt des gesamten Bildschirms. Auf diese Weise können Sie die Sichtbarkeit von sensiblen Informationen einschränken und sicherstellen, dass nur das Notwendige geteilt wird.

Überlegen Sie, ob das Teilen von Anwendungen oder des Bildschirms wirklich notwendig ist, und ob alle Teilnehmer im Meeting Zugriff auf die angezeigten Informationen haben sollten. Vermeiden Sie das Teilen, wenn es nicht erforderlich ist, um Risiken grundsätzlich zu minimieren.

Beenden des Screen-Sharing nach Bedarf: Beenden Sie das Teilen des Bildschirms, sobald es nicht mehr erforderlich ist, um sensible Informationen zu schützen und z.B. die Erstellung von Screenshots zu vermeiden.

3.9.9 Meeting beenden

Sollen Inhalte eines Meetings (Dateien, Aufnahme, Chat-Informationen, usw.) nach der Beendigung nicht mehr jedem Teilnehmer zur Verfügung stehen, muss gewartet werden, bis alle Teilnehmer das Meeting verlassen haben und der Zugriff auf das Meeting, für den/die jeweiligen Meeting-Teilnehmer entfernt werden. Sollten sich Informationen im Chat befinden, welche nach Beendigung nicht mehr zugreifbar sein sollten, muss der Chat-Inhalt gelöscht werden.

Nach Beendigung einer Video-Konferenz mit gemeinsam genutzten Geräten, z. B. Raumsystemen, muss der Nutzer am Gerät abgemeldet werden.

Sollten Personen Zugriff auf die Daten eines Meetings nach seiner Beendigung erhalten, müssen diese dem Meeting nachträglich hinzugefügt werden.

3.10 Microsoft Teams – Teams & Kanäle

3.10.1 Namenskonvention

Durch die Verwendung einer klaren, konsistenten und aussagekräftigen Namenskonvention sollen Organisationen und Verwaltung von Microsoft Teams und Kanälen verbessert werden.

Bei der Anlage und Benennung von Microsoft Teams ist bevorzugt folgendes Vorgehen zu wählen:

- Einrichtungskürzel-Teamname

3.10.2 Anlegen neuer Teams

Jeder Mitarbeiter darf neue Teams und darin enthaltenen Kanäle anlegen. Durch Anlegen eines Teams wird man automatisch zum Besitzer dieses Teams.

Besitzer haben die wichtige Aufgabe, den Zugriff für weitere Mitglieder zu regulieren, also (weitere) Mitglieder in dieses Microsoft Team aufzunehmen. Ein aktives Eintreten eines Benutzers (ohne Genehmigungsverfahren über den Besitzer) in ein Microsoft Team sollte aufgrund der darin ggf. abgelegten Informationen verhindert werden. Besitzer sollten daher bei einer Anfrage eines Benutzers abwägen, ob dieser Zugriff auf sämtliche Informationen, Dateien und Apps innerhalb dieses Teams erhalten darf bzw. muss.

Ebenfalls hat der Besitzer die Aufgabe, eine mögliche Kanalstruktur zu planen und anzulegen, um sicherzustellen, dass vertrauliche Diskussionen in privaten Kanälen stattfinden können, während öffentliche Kanäle für allgemeine Diskussionen genutzt werden.

3.10.3 Hinzufügen weiterer Mitglieder

Besitzer eines Teams haben die Aufgabe, die Mitglieder ihres Teams zu verwalten. Mitglieder, die im Nachgang in ein spezifisches Team aufgenommen werden wollen/müssen, müssen vom Besitzer geprüft und hinzugefügt werden.

Besitzer eines Teams müssen bei einer Beitritts-Anfrage eines Benutzers abwägen, ob dieser Zugriff auf sämtliche Informationen, Dateien und Apps innerhalb dieses Teams erhalten darf bzw. muss.

3.10.4 Gastbenutzer

Die Möglichkeit, Gastbenutzer durch Mitarbeiter einzuladen und in Teams hinzuzufügen, wurde bewusst deaktiviert, um den externen Zugriff auf den Microsoft 365 Tennants zu steuern und das Risiko bzgl. dem externen Zugriff auf Unternehmensdaten zu reduzieren.

3.10.5 Dateiablage

Stellen Sie sicher, dass Zugriffe auf Dateien nur für vorgesehene Personen/Benutzer bestehen. Prüfen Sie die Mitglieder der übergeordneten Teams und gegebenenfalls zusätzliche Freigaben.

Informationen mit einem erhöhten Schutzbedarf, wie beispielsweise personenbezogene Daten gemäß Artikel 9 der Datenschutz-Grundverordnung (DSGVO), dürfen nicht abgelegt oder verarbeitet werden.

3.10.6 Auflösen eines Microsoft Teams

Bevor ein Team in Teams aufgelöst wird, sollten alle wichtigen Daten, Dateien und Informationen gesichert werden. Dies kann durch das Herunterladen von Dateien, das Exportieren von Chat-Verläufen oder das Speichern von wichtigen Informationen erfolgen. Außerdem muss geprüft werden, dass keine laufenden Verpflichtungen oder Projekte im Team vorhanden sind, die möglicherweise abgeschlossen oder an andere Teams übertragen werden müssen. Verantwortlich ist hier der Team-Besitzer.

Zudem müssen alle Teammitglieder über die Auflösung des Teams durch den Besitzer informiert werden. Es ist wichtig sicherzustellen, dass die Mitglieder über alternative Kommunikationskanäle informiert werden, falls sie noch benötigt werden.

Löschen Sie im Anschluss alle nicht mehr benötigten Dateien, Daten und Informationen aus dem Team, um sicherzustellen, dass keine vertraulichen oder sensiblen Informationen zurückbleiben.

Führen Sie die notwendigen Schritte durch, um das Team offiziell aufzulösen. Dies umfasst, das Entfernen aller Mitglieder und das Löschen des Teams selbst.

Inaktive Teams werden darüber hinaus automatisch nach 180 Tagen gelöscht. 30 Tage, 15 Tage und 1 Tag vor der Löschung werden Benachrichtigungen mit Optionen zur Verlängerung per E-Mail an die Team-Besitzer gesendet.

3.11 Microsoft Teams – Apps

Um die Sicherheit und den Datenschutz innerhalb von Microsoft Teams zu gewährleisten, wird die Nutzung von Apps auf die nativen Microsoft-Apps durch die Systemadministratoren beschränkt, während Drittanbieter-Apps deaktiviert sind.

Diese Maßnahme wird aus mehreren Gründen durchgeführt. Erstens können Drittanbieter-Apps potenzielle Sicherheitsrisiken darstellen, da sie möglicherweise Schwachstellen aufweisen, die von Angreifern ausgenutzt werden könnten. Durch die Begrenzung auf native Microsoft-Apps wird das Risiko von Sicherheitslücken minimiert. Zweitens könnten Drittanbieter-Apps Zugriff auf sensible Daten haben, die innerhalb von Microsoft Teams ausgetauscht werden. Die Beschränkung auf native Microsoft-Apps reduziert das Risiko von Datenschutzverletzungen, da der Datenaustausch auf vertrauenswürdige und geprüfte Anwendungen beschränkt ist. Außerdem sind native Microsoft-Apps eng in Microsoft Teams integriert und wurden speziell entwickelt, um eine nahtlose und zuverlässige Benutzererfahrung zu gewährleisten. Dies trägt zur Kompatibilität und Zuverlässigkeit der Plattform bei.

Sollten darüber hinaus Apps innerhalb von Microsoft Teams benötigt werden, ist dies mit der IT zu besprechen und im Anschluss sowohl Sicherheits-, als auch Datenschutztechnisch (via Datenschutzbeauftragtem) zu prüfen.

Der Ablauf ist regelmäßig wie folgt:

1) TU-Mitarbeiter fordert eine App an.
2) Eine Prüfung auf Plausibilität der Anfrage wird in erster Sichtung durchgeführt. Gegebenenfalls ist im Dialog mit der anfordernden Person der abzudeckende Anwendungsfall zu erörtern bzw. mit Fachabteilungen abzustimmen.
3) Sofern eine App-Nutzung kostenpflichtig ist, ist die Frage zu erörtern, wer anfallende Kosten trägt.
4) Zu definieren ist, welcher Nutzerkreis zum Zugriff auf die App berechtigt werden soll bzw. kann.
5) Nach positiver Klärung übergibt das Rechenzentrum die Anfrage an die Prüfung durch den Datenschutzbeauftragten. Falls in Schritt 2 bereits kritische Aspekte festgestellt werden, wird Schritt 5 früher durchlaufen.
6) Sofern eine Datenübertragung an einen Anbieter der App zulässig ist, wird die App zur Nutzung innerhalb des definierten Personenkreises von Administratoren freigegeben.

3.11.1 Microsoft-App „Polls“

Die Nutzung der Teams-App “Polls” ist zulässig und unterstützt die Zusammenarbeit insbesondere in Gremien im Rahmen von Abstimmungen. Bitte beachten Sie, dass bei der Nutzung neben den Umfrageantworten auch Nutzungs- und Metadaten verarbeitet werden; eine vollständige Anonymität kann daher technisch nicht gewährleistet werden. Umfragen sind ausschließlich für arbeitsbezogene Zwecke zu verwenden und dürfen nicht zur Leistungs- oder Verhaltenskontrolle von Beschäftigten eingesetzt werden. Nutzen Sie die Anwendung transparent und nur im Rahmen der vorgesehenen dienstlichen Aufgaben.

3.12 Konferenzraum-Lösungen

3.12.1 Deaktivierung der automatischen Annahme eines Anrufs

Konferenzraumsysteme, die mit Microsoft Teams genutzt werden können, müssen vor der Inbetriebnahme auf eine automatische Anrufannahme-Funktion geprüft werden. Diese Funktion ist wenn vorhanden zu deaktivieren. Die Überprüfung dient dazu, sicherzustellen, dass die Konferenzraumsysteme keine automatische Annahme von Anrufen durchführen, die möglicherweise unerwünschte oder unerwartete Zugriffe auf Informationen ermöglichen könnten. Durch diese Prüfung wird die Sicherheit und Integrität der Konferenzraumsysteme gewährleistet und das Risiko unerwünschter Zugriffe auf Informationen minimiert.

3.12.2 Deaktivierung nicht benötigter Dienste

Die Konferenzraumsysteme, die für die Nutzung mit Microsoft Teams vorgesehen sind, wurden gründlich geprüft, um sicherzustellen, dass sie den Sicherheitsanforderungen entsprechen. Als Teil dieser Prüfung wurden nicht benötigte Dienste und Funktionen deaktiviert. Dieser Schritt ist entscheidend, um die Angriffsfläche zu minimieren und potenzielle Sicherheitsrisiken zu reduzieren.

Darüber hinaus ermöglicht die Deaktivierung nicht benötigter Dienste eine effizientere Ressourcennutzung und verbessert die Leistung der Konferenzraumsysteme insgesamt. Dies trägt dazu bei, eine reibungslose und zuverlässige Nutzung von Microsoft Teams während der Meetings und Konferenzen zu gewährleisten.

3.13 Datensicherung

In M365/Teams abgelegte Daten werden zum aktuellen Zeitpunkt nicht vom Rechenzentrum gesichert. Wenn eine Datensicherung gewünscht / benötigt wird, muss dies durch einen Besitzer des jeweiligen Teams erfolgen. Eine zentrale Backup-Lösung ist in Prüfung.

4 Fqmwo gpvgprtŠhwpi

Verantwortlich für die Pflege und Aktualisierung dieser Sicherheitsrichtlinie ist der ISB. Die Prüfung erfolgt regelmäßig beziehungsweise anlassbezogen, mindestens jährlich.

Änderungsvorschläge können dem ISB formlos mitgeteilt werden.

5 Cpj cpi

Datenschutz: Kategorisierung gemäß LFD Niedersachsen

(Auszug aus https://www.lfd.niedersachsen.de/download/137188/Schutzstufenkonzept_LfD_Niedersachsen_.pdf)

Schutzstufe	Personenbezogene Daten	zum Beispiel	Schwere eines möglichen Schadens
A	die von den Betroffenen frei zugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	geringfügig
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar