IT-Kodex

Beschlossen vom Stadtrat am 12. August 2025

I. Allgemeine Bestimmungen

Art. 1. Zweck

[1] Funktionsfähige Informatiksysteme bilden eine unverzichtbare Grundlage für zahlreiche Geschäfts- und Verwaltungsprozesse. IT-Sicherheit ist deshalb eine wesentliche Voraussetzung:

a) zur Erfüllung des gesetzlichen Auftrages;
b) zur Wahrung des Vertrauens der Öffentlichkeit;
c) zur Sicherung der investierten Werte in Daten und Infrastruktur;
d) zum Schutz von Daten und Programmen vor Missbrauch, Verfälschung und Zerstörung;
e) zur Gewährleistung der Verfügbarkeit und Funktionsfähigkeit der Informatik und der Kommunikationswege.

[2] Um eine angemessene IT-Sicherheit gewährleisten zu können, muss dem Faktor „Mensch“ grosse Beachtung geschenkt werden. Der IT-Kodex unterstützt die Mitarbeitenden dabei, durch verantwortungsbewusstes und sorgfältiges Verhalten einen wesentlichen Beitrag zum Schutz der IT-Systeme und der damit verwalteten Daten zu leisten.

Art. 2. Stellenwert und Geltungsbereich

Der IT-Kodex ist mit der IT-Sicherheitsstrategie der Stadt Chur abgestimmt und für alle Mitarbeitenden, die dem städtischen Personalrecht unterliegen, verbindlich. Er bildet einen integralen Bestandteil des Arbeitsvertrags.

Art. 3. Verantwortlichkeiten

[1] Die Informatik der Stadt Chur (ITSC) informiert regelmässig über aktuelle Gefahren und Sicherheitsvorfälle. Alle Mitarbeitenden sind verpflichtet, diese Informationen aufmerksam zu lesen und die darin enthaltenen Empfehlungen und Anweisungen umzusetzen.

[2] Führungspersonen stellen sicher, dass den Mitarbeitenden der Inhalt des IT-Kodex bekannt ist. Sie weisen regelmässig auf sicherheitsrelevante Aspekte hin und fördern das sicherheitsbewusste Verhalten im Arbeitsalltag.

[3] Alle Mitarbeitenden sind verpflichtet, den IT-Kodex korrekt und vollständig einzuhalten und die Datenschutzvorgaben im Rahmen ihres Aufgabenbereiches zu befolgen. Sie tragen die Verantwortung, sich eigenständig und regelmässig über die Anforderungen der Informationssicherheit und den sicheren Umgang mit Informatikmitteln zu informieren.

Art. 4. Unterstützung

Die Mitarbeitenden sind verpflichtet, bei Unklarheiten im Umgang mit dem IT-Kodex oder mit den Informatiksystemen die ITSC zu kontaktieren. Entsprechende Anfragen sind über das Serviceportal der ITSC zu erfassen.

Art. 5. Verstösse

[1] Verstösse gegen den IT-Kodex gefährden die Informationssicherheit und damit einen wesentlichen Wertbestand der Organisation. Sie können den ordnungsgemässen Ablauf der Geschäftsprozesse erheblich beeinträchtigen.

[2] Verstösse können personalrechtliche Konsequenzen bis hin zur Auflösung des Arbeitsverhältnisses nach sich ziehen. Schwerwiegende Verstösse (z. B. Verletzung des Urheberrechts, des Persönlichkeitsrechts, des Datenschutzes oder die Preisgabe von Dienstgeheimnissen) können zudem zivil- und/oder strafrechtliche Folgen haben.

Art. 6. Kontrolle

[1] Bestehen konkrete Anhaltspunkte für einen Verstoss gegen den IT-Kodex, kann die ITSC weitergehende Kontrollen der Nutzung der IT-Systeme anordnen. Im Ereignisfall informiert die ITSC den Informationssicherheitsbeauftragten (ISB), den Rechtsdienst und die Personaldienste über den Vorfall.

[2] Für das Öffnen persönlicher E-Mails und persönlicher Daten ist vorgängig die Einwilligung der betroffenen Person einzuholen. Vorbehalten bleibt der Rechtsweg.

Art. 7. Abweichungen vom IT-Kodex

Abweichungen vom IT-Kodex sind im Einzelfall möglich, bedürfen jedoch der schriftlichen Form und müssen durch den zuständigen Data Owner und die ITSC genehmigt werden.

II. Definition der Datenarten

Art. 8. Geschäftsdaten

Geschäftsdaten sind sämtliche Daten der Arbeitgeberin, die im Rahmen der dienstlichen Tätigkeit entstehen oder verwendet werden. Dazu gehören insbesondere Daten zu:

a) Verwaltungs- und Geschäftsvorgängen;
b) Kunden-/Klienten- oder Bürgerbeziehungen;
c) Bildungswesen;
d) Personalwesen;
e) kooperierenden Stellen ausserhalb des Verwaltungs-/Geschäftsbereiches;

f) Geschäftspartnern;
g) Projekten;
h) Finanzwesen;
i) Verträgen und rechtlichen Dokumenten.

Art. 9. Vertrauliche Geschäftsdaten

Vertrauliche Geschäftsdaten sind Daten, die aufgrund ihres Inhalts besonders schützenswert sind. Dies gilt insbesondere für Daten:
a) die nicht öffentlich zugänglich sind;
b) deren Informationsgehalt dem Amts- oder Dienstgeheimnis unterliegt;
c) deren Informationsgehalt unter die Bestimmungen des Persönlichkeitsschutzes sowie der eidgenössischen und kantonalen Datenschutzgesetzgebung fällt.

Art. 10. Persönliche Geschäftsdaten

Persönliche Geschäftsdaten sind Daten, die im Zusammenhang mit der dienstlichen Tätigkeit stehen, aber für einzelne Mitarbeitende persönlich bestimmt sind. Dazu zählen beispielsweise die persönliche Mailbox (die auf den Namen des Mitarbeitenden lautende Mailbox), persönliche Notizen, Spesenabrechnungen oder Unterlagen zur Vorbereitung von Mitarbeitergesprächen.

Art. 11. Private Daten

Private Daten sind alle Informationen, die keinen Bezug zur dienstlichen Tätigkeit oder zur Arbeitgeberin haben und ausschliesslich dem privaten Gebrauch der Mitarbeitenden dienen.

III. Aufbau der Datenspeicherung

Die Datenspeicherung ist wie in Abbildung 1dargestellt aufgebaut.

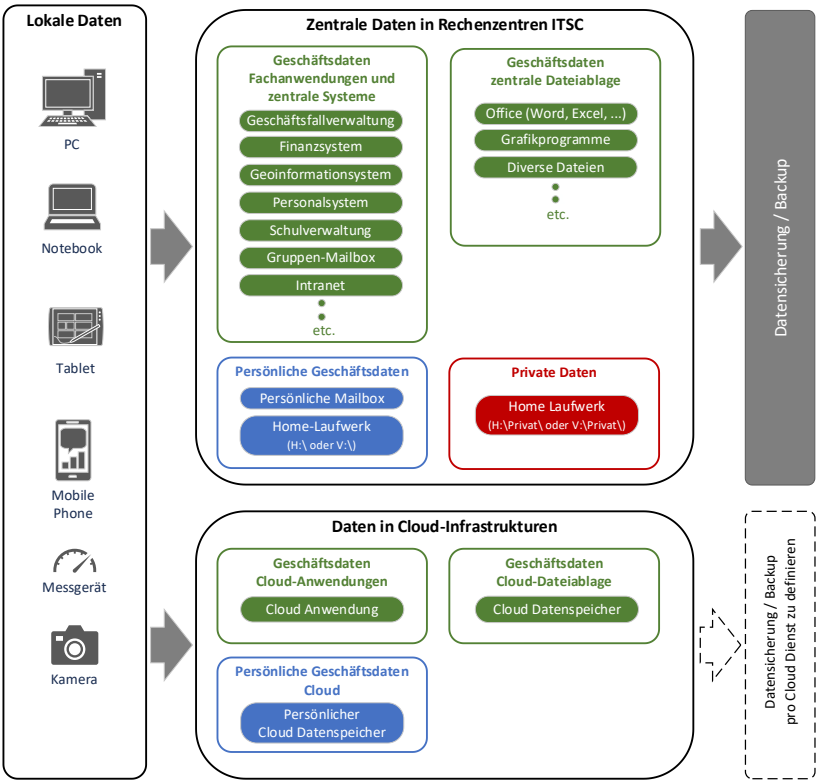

Abbildung 1: Aufbau Datenspeicherung

Art. 12. Zentrale Daten in Rechenzentren der ITSC

Die Daten werden auf den IT-Systemen der ITSC gespeichert. Sie unterliegen dem Datensicherungskonzept der ITSC und werden regelmässig in einem geregelten Verfahren gesichert. Folgende Arten von zentralen Daten werden unterschieden:

a) Geschäftsdaten in Fachanwendungen und in zentralen Systemen:

Daten von Geschäftsfallverwaltung (CMI), Fachanwendungen (Finanzwesen, Personalwesen, Schulverwaltung etc.) und zentralen Systemen (Intranet, Gruppen-Mailboxen).

b) Geschäftsdaten zentrale Dateiablage:

Zentrale Dateiablage für E-Mails und Dateien (Office-Dokumente, PDF-Dateien, Bilder etc.), die im Zusammenhang mit Geschäftsvorgängen stehen.

c) Persönliche Geschäftsdaten:

1. Persönliche Mailbox des Mitarbeitenden für den geschäftlichen Mailverkehr.
2. Persönliches Home-Laufwerk (H:\ oder V:\) des Mitarbeitenden für die Ablage von persönlichen Geschäftsdaten.
3. Die persönliche Mailbox und das persönliche Home-Laufwerk sind für Dritte nicht zugänglich und werden nach dem Austritt des Mitarbeitenden gelöscht.
4. Der Speicherplatz ist begrenzt und die Nutzung ist auf das notwendige Minimum zu beschränken.

d) Private Daten:

Die Ablage für private Dateien und E-Mails ist in Art. 50 geregelt.

Art. 13. Daten in Cloud-Infrastrukturen

[1] Cloud-Daten werden ausserhalb der Rechenzentren der ITSC beim jeweiligen Cloud-Provider gespeichert. Sie unterliegen in der Regel nicht dem Datensicherungskonzept der ITSC. Folgende Arten von Cloud-Daten werden unterschieden:

a) Geschäftsdaten Cloud-Anwendungen:

Geschäftsdaten, die im Rahmen der Nutzung von Cloud-Anwendungen entstehen und innerhalb dieser gespeichert werden.

b) Geschäftsdaten Cloud-Dateiablage:

Cloud-Speicher zur Ablage von geschäftlichen Dateien.

c) Persönliche Geschäftsdaten Cloud:

1. Persönlicher Cloud-Speicher des Mitarbeitenden (Microsoft OneDrive).
2. Der persönliche Cloud-Speicher ist für Dritte nicht zugänglich und wird nach dem Austritt automatisch durch den Cloud-Provider gelöscht.
3. Der Speicherplatz ist begrenzt und die Nutzung ist auf das notwendige Minimum zu beschränken

[2] Für die Nutzung von Cloud-Anwendungen und Cloud-Speichern gelten die Bestimmungen gemäss Art. 43.

Art. 14. Lokale Daten

Als lokale Daten werden Informationen bezeichnet, die auf Arbeitsplatzrechnern oder mobilen Geräten (Notebook, Tablet, Smartphone etc.) gespeichert werden. Sie entstehen unter anderem durch:

a) das Einlesen von USB-Speichermedien (z. B. aus Fotokameras, Messgeräten);

b) die Nutzung lokaler Anwendungen im Offline-Modus (d. h. ohne Netzwerkverbindung);
c) die Speicherung von Daten auf lokalen Datenträgern.

IV. Umgang mit Daten – korrekte Speicherung

Art. 15. Bearbeiten und Speichern von geschäftlichen Daten

[1] Die Bearbeitung und Speicherung von Geschäftsdaten ist ausschliesslich mittels Anwendungen oder Cloud-Plattformen gestattet, welche von der ITSC für diesen Zweck freigegeben wurden.

[2] Die Speicherung von Geschäftsdaten hat grundsätzlich nach folgender Prioritätenordnung zu erfolgen:

a) Erste Priorität: In der Geschäftsfallverwaltung (CMI) oder in den dafür vorgesehenen Fachanwendungen (Art. 12 lit a);
b) Zweite Priorität: In der zentralen geschäftlichen Dateiablage (Art. 12 lit b). Die Daten sind unverschlüsselt zu speichern;
c) Dritte Priorität: In der persönlichen Ablage (Art. 12 lit c), sofern nachvollziehbare Gründe vorliegen, welche eine Speicherung gemäss lit a und b ausschliessen.

[3] E-Mails mit geschäftsrelevanten Inhalten sind gemäss Abs. 2 lit. a und b zu speichern. Als geschäftsrelevant gelten E-Mails, welche einen Bezug zu Geschäftsvorgängen haben und für die Nachvollziehbarkeit dieser Vorgänge relevant sind.

[4] Es ist ausdrücklich untersagt:

a) Private Daten in der geschäftlichen Dateiablage zu speichern. Private E-Mails sind aus der persönlichen Mailbox zu entfernen und entweder gem. Art. 50 abzulegen oder an eine private Mailbox weiterzuleiten;
b) Geschäftliche Daten in der privaten Dateiablage zu speichern.

Art. 16. Unbefugtes Kopieren und Mitnehmen von Geschäftsdaten

Das Kopieren von Geschäftsdaten auf fremde Systeme (z. B. private Computer) sowie das Mitnehmen, Entfernen oder Versenden solcher Daten ausserhalb der ordnungsgemässen Prozesse ist untersagt. Zuwiderhandlungen können strafrechtlich verfolgt werden.

Art. 17. Archivierungspflicht und Archivreglement

Organisationseinheiten, die dem Archivreglement der Stadt Chur und dem kantonalen Gesetz über die Aktenführung und Archivierung unterstehen, haben bei der Ablage und Aufbewahrung von Geschäftsdaten die gesetzlichen Archivierungspflichten einzuhalten. Der Archivierungspflicht ist wie folgt nachzukommen:

a) Die Speicherung in der Geschäftsfallverwaltung (CMI) gewährleistet die rechtskonforme Archivierung gemäss der obengenannten Archivgesetzen;
b) Bei Einführung neuer Fachapplikationen muss für die Archivierungszwecke die selektive Entnahme der archivwürdigen Geschäftsdaten gewährleistet sein. Die Archivierung ist vorgängig mit dem Stadtarchiv zu klären;
c) Bei Verwendung der geschäftlichen Dateiablage ist die Archivierung durch die zuständige Dienststelle oder Abteilung mit dem Stadtarchiv zu klären.

Art. 18. Lokale Datenspeicherung

[1] Die Speicherung geschäftsrelevanter Daten auf lokalen Datenträgern (z. B. PC, Laptop, Tablet) ist nur in Ausnahmefällen und nur für kurze Zeit zulässig. Die Daten sind so rasch wie möglich auf die zentrale Dateiablage zu übertragen.

[2] Lokale Daten sind nicht Bestandteil des Datensicherungskonzepts der ITSC. Die Verantwortung für deren Sicherheit und Verfügbarkeit liegt vollumfänglich bei der nutzenden Person.

[3] Bei einer Neuinstallation eines Geräts (z. B. infolge eines technischen Defekts oder einer Malware-Infektion) gehen lokal gespeicherte Daten unwiderruflich verloren.

[4] Bei Verlust oder Diebstahl des Geräts kann ein unbefugter Zugriff auf lokal gespeicherte Daten nicht ausgeschlossen werden.

Art. 19. Datensynchronisation mit privaten Geräten

[1] Die Synchronisation von geschäftlichen Daten mit privaten Geräten ist grundsätzlich untersagt.

[2] Eine Ausnahme bildet die Synchronisation mit privaten Smartphones und Tablets, sofern diese über einen von der ITSC genehmigten und bereitgestellten Dienst (z. B. E-Mail- und Kalendersynchronisation) erfolgt. Weitere Ausnahmen können von der ITSC ausdrücklich definiert und freigegeben werden.

[3] Die ITSC behält sich das Recht vor, technische Massnahmen zu ergreifen und Konfigurationsrichtlinien auf den privaten Geräten durchzusetzen, um eine angemessene Informationssicherheit zu gewährleisten. Wird diesen Massnahmen oder Richtlinien nicht zugestimmt, wird die Datensynchronisation unterbunden.

[4] Vor der Weitergabe oder der Entsorgung eines privaten Geräts (z. B. Smartphone, Tablet oder PC) sind alle geschäftlichen Daten (z. B. E-Mails, Kontakte, Kalender, Dokumente) vollständig zu löschen. Das Gerät ist auf die Werkseinstellungen zurückzusetzen (Factory Reset).

[5] Bei Beendigung des Arbeitsverhältnisses sind die Mitarbeitenden verpflichtet, sämtliche geschäftliche Daten auf privaten Geräten unverzüglich zu löschen.

Art. 20. Datenaustausch mit externen Stellen

[1] Der Austausch vertraulicher Daten mit externen Stellen darf ausschliesslich in verschlüsselter Form erfolgen. Für die Verschlüsselung sind ausschliesslich die von der ITSC bereitgestellten oder ausdrücklich autorisierten Mittel und Dienste zu verwenden.

[2] Benötigt der Empfänger der Daten für die Entschlüsselung ein Passwort, so ist dieses über einen separaten Kanal mitzuteilen (z. B. telefonisch oder per SMS).

Art. 21. Termine mit vertraulichen Daten

Private Termine und Termine mit sensiblen Informationen sind zur Wahrung der Vertraulichkeit im Kalender als "privat" zu kennzeichnen.

Art. 22. Grundsätze für den Zugriff auf persönliche Daten/Mailbox

[1] Benötigt die Arbeitgeberin aus geschäftlichen Gründen Zugriff auf die persönliche Datenablage eines Mitarbeitenden (Mailbox, Home-Laufwerk, Cloud-Speicher), ist vorgängig die schriftliche Einwilligung des betroffenen Mitarbeitenden einzuholen. Vorbehalten bleibt der Rechtsweg.

[2] Um Zugriffskonflikte zu vermeiden, sind geschäftsrelevante Daten ausschliesslich an den in Art. 12 lit. a und b definierten Ablageorten zu speichern.

V. IT-Sicherheit

Art. 23. Grundsätzliches

[1] Mitarbeitende tragen die Verantwortung für alle Zugriffe auf IT- und Kommunikationsmittel, Anwendungen und Daten, die unter ihrer persönlichen Benutzerkennung erfolgen.

[2] Es ist untersagt, IT-Sicherheitsvorkehrungen auszuschalten, zu umgehen oder dies zu versuchen.

[3] Der Anschluss fremder Geräte an das Netzwerk der ITSC (ChurNet) ist grundsätzlich untersagt. Ausgenommen sind Geräte, die von der ITSC ausdrücklich freigegeben wurden, sowie Verbindungen über speziell dafür vorgesehene Netzwerke wie z. B. das Public WLAN.

[4] Die Verwendung der IT-Infrastruktur im Zusammenhang mit rassistischen, gewalttätigen, sexistischen oder anderen illegalen Inhalten ist verboten.

Art. 24. Verhalten bei vermutetem Befall mit Viren oder Schadsoftware

[1] Schadsoftware kann grossen Schaden anrichten. Trotz technischer Schutzmassnahmen bleiben Restrisiken bestehen. Deshalb ist ein sorgfältiger Umgang mit IT-Systemen unerlässlich.

[2] Bei ungewöhnlichem Verhalten oder verdächtigen Fehlermeldungen sind Mitarbeitende angewiesen, das Gerät sofort vom Netzwerk zu trennen (Netzwerkkabel ziehen, WLAN deaktivieren) oder auszuschalten und umgehend den ITSC-Servicedesk zu informieren.

Art. 25. Meldepflicht bei sicherheitsrelevanten Vorfällen

[1] Mitarbeitende sind verpflichtet, sicherheitsrelevante Vorfälle sowie entsprechende Verdachtsmomente unverzüglich dem ITSC-Servicedesk zu melden. Dazu zählen insbesondere:

a) Malware-Befall (z. B. Viren, Trojaner);
b) Offenlegung oder unbefugter Zugriff auf Daten;
c) Datenverlust;
d) Diebstahl von IT-Geräten oder Datenträgern;
e) sonstige ungewöhnliche oder verdächtige Vorkommnisse im IT-Betrieb.

[2] Nur durch eine rasche Meldung können Gegenmassnahmen zeitnah eingeleitet und potenzielle Schäden wirksam begrenzt werden.

Art. 26. Anmeldedaten für IT-Lösungen der ITSC

[1] Die IT-Anwendungen, welche durch die ITSC betrieben werden, beinhalten verschiedene Massnahmen, um die Geschäftsdaten zu schützen. Die Mitarbeitenden werden durch ihre persönlichen Zugangsdaten (Login) zur Nutzung der ihnen zugewiesenen Anwendungen und Daten autorisiert. Bei der Nutzung der Zugangsdaten ist folgendes zu beachten:

a) Mitarbeitende sind verpflichtet, Anmeldenamen und Passwort geheim zu halten. Das Passwort darf niemals anderen Personen bekannt geben werden, auch nicht dem IT-Support;
b) es ist nicht erlaubt, Anmeldenamen und Passwort von anderen Personen zu benutzen;
c) Passwörter müssen den geltenden Passwortrichtlinien entsprechen und dürfen nicht leicht zu erraten sein (mindestens 12 Zeichen, bestehend aus Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen);
d) bei Anzeichen einer möglichen Kompromittierung (z. B. Passwort offengelegt oder erraten), ist das Passwort sofort zu ändern und der Vorfall dem ITSC-Servicedesk zu melden;
e) geschäftliche Passwörter müssen sich von privaten Passwörtern deutlich unterscheiden;
f) nach Beendigung des Arbeitsverhältnisses sind der Arbeitgeberin auf Verlangen alle Passwörter im Zusammenhang mit den geschäftlichen Anwendungen und Dateiablagen bekannt zu geben.

[2] Mitarbeitende, die ihren Benutzernamen oder ihr Passwort vergessen haben, können sich telefonisch an den ITSC-Servicedesk wenden.

Art. 27. Anmeldedaten für externe Anwendungen

[1] Die geschäftliche E-Mail-Adresse darf für die Anmeldung bei externen Anwendungen (z. B. Webdienste, Webportale) nur verwendet werden, wenn dies für die Ausübung der geschäftlichen Tätigkeit erforderlich ist.

[2] Für externe Anwendungen darf niemals dasselbe Passwort verwendet werden wie für die IT-Lösungen der ITSC. Folgende Vorgaben sind zu berücksichtigen:

a) Pro Dienst muss ein separates Passwort verwendet werden;
b) es sind Passwörter zu wählen, die den gängigen Passwortrichtlinien entsprechen;
c) zusätzliche Sicherheitsfunktionen (z. B. Zwei-Faktor-Authentifizierung) des jeweiligen Diensteanbieters sind zu nutzen, sofern diese angeboten werden.

Art. 28. Verlassen des Arbeitsplatzes

[1] Beim Verlassen des Arbeitsplatzes ist die Bildschirmsperre zu aktivieren oder eine Abmeldung vom System vorzunehmen.

[2] Nach Arbeitsschluss ist die Arbeitsstation inklusive Bildschirm ordnungsgemäss herunterzufahren.

Art. 29. USB-Speichermedien/Speicherkarten

Der Einsatz mobiler Datenträger (z. B. USB-Sticks, Speicherkarten) ist nur in Ausnahmefällen gestattet und erfordert eine vorherige Freigabe durch die ITSC (Abweichung vom Standard). Vor der jeweiligen Verwendung müssen mobile Datenträger auf Viren und andere Schadsoftware geprüft werden.

Art. 30. Mobiles Arbeiten

[1] Beim mobilen Arbeiten und im Home-Office sind die folgenden Punkte einzuhalten:

a) Es dürfen nur IT-Mittel genutzt werden, welche von der ITSC für diesen Zweck zur Verfügung gestellt werden (z. B. Remote-Zugang oder Notebook der ITSC);
b) sämtliche Daten und Informationen sind angemessen zu schützen und der Arbeitsplatz muss so eingerichtet sein, dass Unbefugte keinen Zugang zu geschäftlichen Daten erhalten;
c) beim mobilen Arbeiten ist darauf zu achten, dass Dritte den Bildschirm nicht einsehen können, insbesondere in öffentlichen Verkehrsmitteln;
d) geschäftliche IT-Mittel dürfen nicht unbeaufsichtigt bleiben und müssen sicher aufbewahrt werden;
e) für die anvertrauten Wertbestände (Hardware und Daten auf dem System) sind die Mitarbeitenden persönlich verantwortlich. Der Verlust eines mobilen Arbeitsgerätes ist unverzüglich dem ITSC-Servicedesk zu melden;

f) die ITSC leistet keinen Support für private Geräte.

[2] Ebenfalls ist die separate „Richtlinie mobile Endgeräte“ als verbindlich zu beachten.

Art. 31. Social Engineering

[1] Mitarbeitende sollten sich der Gefahren des Social Engineering stets bewusst sein und sich nicht aus Hilfsbereitschaft, Gutgläubigkeit oder Angst vor Konsequenzen dazu verleiten lassen, die IT-Sicherheit zu vernachlässigen. Besondere Vorsicht ist geboten, wenn versucht wird, Mitarbeitende zu unerlaubten Handlungen zu verleiten, wie z. B.:

a) Weitergabe von vertraulichen Informationen;
b) Bekanntgabe von Passwörtern;
c) Erteilen von Zugriffen auf IT-Systeme;
d) Gewähren des Zuganges zu Büroräumlichkeiten.

[2] Unbefugten Personen darf weder Zugang zu IT-Systemen noch Einsicht in schützenswerte Daten und Geschäftsprozesse gewährt werden.

Art. 32. Ausweispflicht beim Unterhalt an IT-Systemen

[1] Der Unterhalt an IT-Systemen, sowie deren Austausch oder Entsorgung erfolgt ausschliesslich durch Mitarbeitende der ITSC oder durch von der ITSC beauftragte Lieferanten. Unbekannten oder nicht identifizierten Personen darf niemals Zugriff auf IT-Systeme gewährt werden.

[2] Personen, die berechtigt sind, Wartungsarbeiten an IT-Systemen durchzuführen, müssen einen sichtbaren Ausweis auf sich tragen. Wird kein Ausweis sichtbar getragen, ist die betreffende Person darauf anzusprechen. Wenn kein Ausweis vorgelegt werden kann, muss durch eine Rückfrage bei der ITSC geklärt werden, ob die Person im Auftrag der ITSC handelt.

Art. 33. Protokollierung und Auswertung von Logdaten

[1] Zur Gewährleistung der technischen IT-Sicherheit sowie für die Kapazitätsplanung werden die Nutzung der Informatik- und Kommunikationsmittel automatisiert protokolliert und ausgewertet (z. B. Netzwerkauslastung oder die Speicherbelegung). Eine vertiefte Auswertung erfolgt, wenn ein sicherheitsrelevanter Vorfall eingetreten ist, eine Störung des Betriebs vorliegt, oder Hinweise auf einen möglichen Vorfall bestehen.

[2] Allfällige private Nutzungen können mitprotokolliert werden, da aus technischen Gründen keine Trennung zwischen privater und geschäftlicher Nutzung möglich ist.

Art. 34. Beschaffung, Nutzung und Entsorgung von Informatikmitteln

[1] Die Beschaffung und Installation von Hard- und Software erfolgt ausschliesslich durch die ITSC. Die Nutzung jeglicher Hard- und Software, welche nicht durch die ITSC freigegeben wurde, ist untersagt.

[2] Jegliche Manipulationen an Hard- und Software sind untersagt. Die installierte Software darf weder kopiert noch auf andere Geräte übertragen, weitergegeben oder modifiziert werden.

[3] Die Entsorgung von IT-Geräten erfolgt ausschliesslich durch die ITSC, welche die ordnungsgemässe Löschung der Daten sicherstellt.

VI. Nutzung der E-Mail-Dienste

Art. 35. Gefährliche E-Mails

[1] Gefährliche E-Mails sind Nachrichten, die aufgrund ihres Inhalts oder bestimmter Merkmale als verdächtig oder potenziell betrügerisch gelten. Sie können verschiedene Ziele verfolgen, wie den Diebstahl sensibler Daten (z. B. Phishing-Mails) oder die Verbreitung von Schadsoftware (z. B. Malware, Ransomware). Solche Schadsoftware kann Daten verschlüsseln oder unlesbar machen und erheblichen Schaden verursachen.

[2] E-Mails können bestimmte Hinweise enthalten, die auf eine fehlende Vertrauenswürdigkeit schliessen lassen:

a) Der Absender ist unbekannt, und es besteht kein erkennbarer geschäftlicher Zusammenhang;
b) der Absender ist bekannt, aber der Inhalt der E-Mail weist keinen Bezug zu einem geschäftlichen Vorgang auf;
c) ein geschäftlicher Zusammenhang ist zwar erkennbar, jedoch ist der Kommunikationskanal oder der Zeitpunkt der E-Mail ungewöhnlich;
d) es sind dringende Aufforderungen zu sofortigen Massnahmen enthalten, wie z. B. Zahlungen auszuführen oder Bildschirmfreigaben zu erteilen;
e) die E-Mail enthält unerwartet zugesandte Dateianhänge;
f) die E-Mail enthält Links zu scheinbar offiziellen Webseiten, die zur Eingabe vertraulicher Informationen (z. B. Passwörter, Zahlungsdaten) auffordern;
g) Rechtschreibung und Grammatik sind fehlerhaft.

[3] Bei Unsicherheit über die Echtheit einer E-Mail ist telefonisch beim vermeintlichen Absender nachzufragen oder die E-Mail ist zur Überprüfung an die ITSC weiterzuleiten.

Art. 36. Versand vertraulicher Informationen per Mail

[1] E-Mails werden standardmässig unverschlüsselt übertragen und können deshalb auf jedem für die Übertragung involvierten Mail-Gateway mitgelesen und verändert werden. Deshalb dürfen vertrauliche Informationen nicht ohne

spezielle Schutzmassnahmen per E-Mail an externe Empfänger versendet werden.

[2] Die Übertragung vertraulicher Daten an interne E-Mail-Adressen ist zulässig, da diese nicht über das öffentliche Internet erfolgt. Alle IT-Service-Bezüger der ITSC (Stadt Chur, IBC, Bus & Service AG, Region Plessur usw.), sowie Empfänger der kantonalen Verwaltung Graubünden (E-Mail-Adresse mit xx@xx.gr.ch) gelten dabei als interne Empfänger, weil diese über vertrauenswürdige Netzwerke direkt angebunden sind.

[3] Für den Versand von vertraulichen Informationen via E-Mail an externe Empfänger stellt die ITSC separate Werkzeuge zur Verfügung. Informationen hierzu sind im Intranet verfügbar oder können beim ITSC-Servicedesk eingeholt werden.

Art. 37. Abwesenheiten

[1] Bei Abwesenheit ist eine Abwesenheitsnotiz zu aktivieren, die über die Dauer der Abwesenheit und die Vertretung informiert.

[2] Im Falle der Einrichtung einer automatischen Weiterleitung von E-Mails oder der Leseberechtigung Dritter für die persönliche Mailbox sind der Datenschutz und das Amtsgeheimnis zu gewährleisten.

Art. 38. Aufbewahrungspflicht geschäftsrelevanter E-Mails

Als geschäftsrelevant gelten E-Mails, die einen direkten Bezug zu Geschäftsvorgängen haben und für deren Nachvollziehbarkeit erforderlich sind. Solche E-Mails einschliesslich Anhängen sind an den in Art. 12 lit. a und b genannten Ablageorten zu speichern.

Art. 39. Umgang mit E-Mail-Speicherplatz

Zur Optimierung der Netzwerk- und Kapazitätsressourcen wird der zur Verfügung stehende Speicherplatz mittels Kontingenten limitiert. Die Zuteilung und Überwachung von Speicherplatz erfolgt durch die ITSC.

VII. Nutzung des Internets

Art. 40. Eigene Identifikation im Internet

Bei der Nutzung des Internetzugangs vertreten Mitarbeitende die Arbeitgeberin. Sie sind angehalten, ihren korrekten Namen und die offizielle Adresse zu verwenden. In Ausnahmefällen (z. B. aus Sicherheitsgründen) kann auf die Verwendung von Pseudonymen zurückgegriffen werden, sofern dies mit den Vorgaben der Arbeitgeberin abgestimmt ist.

Art. 41. Bezug und Publikation von Informationen

Es dürfen keine Inhalte publiziert oder konsumiert werden, welche gegen die Rechtsordnung verstossen.

Art. 42. Software aus dem Internet

Das eigenständige Herunterladen und Nutzen von Software aus dem Internet sind untersagt. Wird Software aus dem Internet für dienstliche Zwecke benötigt, ist der ITSC-Servicedesk zu kontaktieren.

Art. 43. Nutzung von Cloud-Diensten/SaaS (Software as a Service)

[1] Die Nutzung von Cloud-Diensten für geschäftliche Zwecke ist grundsätzlich untersagt, sofern sie nicht ausdrücklich von der Arbeitgeberin bereitgestellt oder genehmigt wurden. Vor der Einführung oder Nutzung eines Cloud-Dienstes sind die Verantwortlichkeiten, kommerziellen Aspekte und Sicherheitsanforderungen in Abstimmung mit der ITSC verbindlich zu regeln.

[2] Der Cloud-Nutzer (bzw. die nutzende Organisation) trägt die Verantwortung für die Daten und die Einhaltung aller gesetzlichen Vorgaben, insbesondere des Datenschutzgesetzes.

[3] Der Cloud-Nutzer (bzw. die nutzende Organisation) trägt die Verantwortung für die Informationssicherheit und Datensicherung, sofern keine anderweitige Regelung besteht.

[4] Die geltenden Leitlinien, Merkblätter und Weisungen der ITSC bezüglich der Nutzung bestimmter Cloud-Dienste sind zwingend zu beachten.

Art. 44. Umgang mit vertraulichen Daten im Internet

[1] Die Eingabe oder Weitergabe vertraulicher oder schützenswerter Daten über Internetdienste ist untersagt. Insbesondere dürfen keine vertraulichen Daten in Suchmaschinen, Übersetzungsdienste, Chat-Dienste oder Dienste mit künstlicher Intelligenz (KI) eingegeben werden. Es besteht das Risiko, dass diese Daten vom Dienstanbieter für andere Zwecke, wie beispielsweise das Training von KI-Modellen, genutzt werden.

[2] Die nutzende Person ist dafür verantwortlich zu prüfen, ob die Nutzung des Dienstes für den vorgesehenen Zweck zulässig ist und den gesetzlichen Vorgaben, insbesondere dem Datenschutzgesetz, entspricht.

Art. 45. Streaming

Die Nutzung von Streaming-Diensten (z. B. Radio, Video) verursacht einen kontinuierlichen Datenstrom. Dies kann zu einer Überlastung des IT-Netzes der ITSC führen. Streaming-Angebote sind daher auf die geschäftliche Nutzung zu beschränken.

Art. 46. Nutzung von Chat- und Messenger-Diensten

[1] Chat- und Messenger-Dienste (z. B. MS Teams, Facebook Messenger, LinkedIn Chat, WhatsApp) sind anfällig für verschiedene Arten von Betrugsversuchen wie Phishing und die Verbreitung von Malware. Bei der Nutzung solcher Dienste ist grundsätzlich die gleiche Vorsicht wie im E-Mail-Verkehr walten zu lassen, um sich vor Betrugsversuchen und Sicherheitsrisiken zu schützen.

[2] Bei der Verwendung von Chat- und Messenger-Diensten sind folgende Grundsätze zu beachten:

a) keine Links in verdächtigen oder unerwarteten Nachrichten anklicken;
b) keine empfangenen Dateianhänge ohne Prüfung öffnen;
c) unbekannten Absendern nicht blind vertrauen, denn das Benutzerprofil könnte gefälscht sein;
d) bei auffällig dringenden oder ungewöhnlichen Aufforderungen (z. B. sofortiges Handeln, Geldüberweisungen) ist besondere Vorsicht geboten;
e) keine vertraulichen oder personenbezogenen Informationen übermitteln;
f) die Datenschutzbestimmungen des genutzten Dienstes sind zu prüfen, ebenso die Zulässigkeit der Nutzung für den vorgesehenen geschäftlichen Zweck.

VIII. Rechtliches

Art. 47. Urheberrechte

[1] Daten, Programme und andere digitale Inhalte unterliegen urheberrechtlichen, lizenzrechtlichen oder anderen rechtlichen Schutzbestimmungen. Mitarbeitende sind verpflichtet, diese Vorgaben einzuhalten und insbesondere keine unrechtmässige Vervielfältigung, Nutzung oder Weitergabe vorzunehmen.

[2] Beim Kopieren oder Verwenden von Inhalten aus dem Internet (z. B. Texte, Bilder, Grafiken) sind die damit verbundenen Urheberrechte sowie Quellenangaben zu berücksichtigen. Eine Verwendung ohne klare rechtliche Grundlage oder Nutzungsrecht ist untersagt.

[3] Die Nutzungsrechte an Erfindungen, Entdeckungen, Ideen, Konzepten, Methoden und Softwareprogrammen, die im Zusammenhang mit IT-Lösungen der Arbeitgeberin erarbeitet wurden, sind im Eigentum der Arbeitgeberin.

Art. 48. Verträge im Internet

Im Internet können rechtsgültige Verträge abgeschlossen werden:

a) Mitarbeitende haben zu berücksichtigen, dass sie nur im Rahmen ihrer Befugnis (u. a. Kompetenzregelung) für die Arbeitgeberin rechtsverbindliche Verträge eingehen können;

b) Mitarbeitende sind dazu verpflichtet, Angebote in elektronischer Form mit Sorgfalt zu prüfen. Es ist sicherzustellen, dass alle Geschäftsbedingungen bekannt und nachvollziehbar vorhanden sind.

IX. Private Nutzung von IT-Lösungen der Arbeitgeberin

Art. 49. Grundsätzliches

[1] Die IT-Lösungen der ITSC sind grundsätzlich für die geschäftliche Nutzung vorgesehen. Im Sinne einer grosszügigen Haltung wird jedoch auf ein absolutes Verbot der privaten Nutzung verzichtet.

[2] Zulässig ist eine gelegentliche, nicht regelmässige private Nutzung, solange diese den regulären IT-Betrieb nicht stört und die eigene Auftragserfüllung sowie die der anderen Mitarbeitenden nicht behindert.

Art. 50. Speicherung von privaten Daten

[1] Grundsätzlich ist auf die Speicherung von privaten Daten zu verzichten. Falls dies im Rahmen der erlaubten privaten Nutzung dennoch notwendig ist, müssen sie im Verzeichnis „Privat" (H:\Privat\ oder V:\Privat\) des Home-Laufwerks gespeichert werden. Dieses Verzeichnis muss durch den Mitarbeitenden selbst erstellt werden.

[2] Vor dem Austritt hat der Mitarbeitende seine privaten Daten zu löschen oder für die weitere Verwendung selbstständig zu sichern. Auf Wunsch händigt die ITSC dem Mitarbeitenden zum Zeitpunkt des Austritts die Daten aus dem privaten Verzeichnis (H:\Privat\ oder V:\Privat\) aus. Andernfalls werden diese Daten nach dem Austritt gelöscht.

[3] Der Speicherplatz für die Ablage privater Daten ist beschränkt. Die Nutzung ist auf das notwendige Minimum zu reduzieren.

Art. 51. Programme

[1] Für die gelegentliche private Nutzung zugelassen sind folgende Standard-Anwendungen: Word, Excel, PowerPoint, Outlook/E-Mail, Internet-Browser, persönlicher Passwortsafe, Programme für die Bildbearbeitung, Telefonie und Kopiergeräte.

[2] Die gelegentliche private Nutzung des Internet-Zugangs zum Zweck der Informationsbeschaffung ist zulässig. Dabei sind die Bestimmungen gemäss Kapitel V. IT-Sicherheit einzuhalten.

[3] Für alle anderen Anwendungen ist die private Nutzung untersagt.

Art. 52. Rechtsanspruch aus privater Nutzung

[1] Durch die private Nutzung der IT-Lösungen der Arbeitgeberin entstehen für den Mitarbeitenden keinerlei Rechtsansprüche gegenüber der Arbeitgeberin.

[2] Die Arbeitgeberin übernimmt keinerlei Haftung für die Verfügbarkeit, die Sicherheit oder die Vertraulichkeit gegenüber Dritten bezüglich der auf Systemen der ITSC gespeicherten privaten Daten.

Art. 53. Datenschutz, Schutz der Privatsphäre

Die Arbeitgeberin hält gegenüber den Mitarbeitenden bezüglich privater Daten die Bestimmungen der Schweizerischen Datenschutzgesetzgebung und des Persönlichkeitsschutzes ein.

X. Glossar

Begriff	Erläuterung
ChurNet	IT-Plattform der Stadt Chur.
Data Owner	Der Data Owner trägt die Verantwortung für die ihm zugeteilte Datensammlung und ist entscheidend für die Gewährleistung der Informationssicherheit. Der Data Owner entscheidet z. B. welche Personen auf die Daten zugreifen und diese bearbeiten dürfen. Aufgrund der Verantwortung sollte die Rolle des Data Owners durch eine Führungsperson wahrgenommen werden (z. B. Dienststellenleiter).
Datenschutz	Datenschutz bezweckt die Wahrung der Persönlichkeitsrechte von natürlichen Personen und greift in die Arbeitsgebiete der IT und der Informationssicherheit ein.
Informations-sicherheits-beauftragter (ISB)	Informationssicherheitsbeauftragter der Informatik der Stadt Chur. Überwacht und unterstützt die Umsetzung der IT-Sicherheitsrichtlinien innerhalb der ITSC.
Informations-sicherheit	Informationssicherheit dient, ungeachtet der Art ihrer Darstellung und Speicherung, dem Schutz bezüglich Vertraulichkeit, Verfügbarkeit und Integrität sämtlicher Informationen.
Mail-Gateway	Ein Mail-Gateway ist ein System, welches den Verkehr von E-Mails überwacht, filtert und kontrolliert, um die Sicherheit und den reibungslosen Ablauf des E-Mail-Verkehrs zu gewährleisten. Es kann Spam-Filter, Virenschutz und Verschlüsselungsfunktionen enthalten.
Malware	Setzt sich aus den englischen Begriffen «malicious» (bösartig) und «Software» zusammen. Malware ist der Oberbegriff für Software, die schädliche Funktionen auf einem Gerät ausführt (wie z.B. Viren, Würmer, Trojaner, Ransomware).
IT-Lösungen	Ein oder mehrere IT-Systeme, welche sich gegenseitig ergänzen bzw. Abhängigkeiten zueinander haben, um einen oder mehrere Geschäftsfälle abzudecken.

ITSC	Informatik der Stadt Chur
Ransomware	Malware, welche Dateien auf einem Gerät sowie auf allfällig verbundenen Netzlaufwerken und Speichermedien (z. B. externe Festplatten, Cloud-Speichern) verschlüsselt und danach Lösegeldzahlungen fordert.
Social Engineering	Angriff, der weniger auf technischem, dafür auf psychologischem Weg erfolgt. Dies ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Um an vertrauliche Informationen zu gelangen, wird sehr oft die Gutgläubigkeit und die Hilfsbereitschaft aber auch die Unsicherheit einer Person ausgenutzt. Von fingierten Telefonanrufen über Personen, die sich als jemand anderes ausgeben, bis hin zu Phishing-Attacken ist vieles möglich.
SaaS (Software as a Service)	SaaS (Software as a Service) ist ein Modell für die Bereitstellung von Software-Anwendungen über das Internet. Bei SaaS-Systemen werden Anwendungen von einem Anbieter gehostet und gewartet, und die Nutzer greifen über das Internet darauf zu, anstatt die Software auf ihren eigenen Computern oder Servern zu installieren. Die Software wird in der Regel als Abonnementsdienst bereitgestellt, was regelmässige Zahlungen an den Anbieter beinhaltet.