STADT
ZOFINGEN

STADTRAT

Kirchplatz 26 / Postfach
4800 Zofingen

T 062 745 71 10

stadtrat@zofingen.ch
www.zofingen.ch

Der Stadtrat Zofingen

an den Einwohnerrat

ER.2023.026

IT-Strategie – Verpflichtungskredit für Umsetzung

Inhalt

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

I Zusammenfassung

Der beantragte Verpflichtungskredit in der Höhe von CHF 1'234'800 ist die finanzielle Grundlage für die gesamtheitliche Erneuerung der IT-Arbeitsplätze der Stadt Zofingen und stützt sich auf die ausgearbeitete IT-Strategie. Sowohl die Arbeitsplätze der Mitarbeitenden wie auch die IT-Infrastruktur für den Betrieb der virtuellen Clients, der Applikationen und Dateiablagen müssen altersbedingt ersetzt werden. Die eingesetzten Softwareversionen der Microsoft-Office Programme stehen nicht mehr unter Softwarewartung und müssen auf neuere Versionen aktualisiert werden.

Durch die fortschreitende digitale Transformation vieler Geschäftsprozesse ändern sich auch in der öffentlichen Verwaltung die Arbeitsweisen und die Form der Zusammenarbeit. Vermehrt wird in Projekten bereichsübergreifend und mit externen Partnern zusammengearbeitet. Diesen Ansprüchen wird mit dem Umstieg auf neue cloudbasierte Dienste und Programme sowie dem Einsatz von mobilen Geräten Rechnung getragen. Die Vorlage leistet somit auch einen wichtigen Beitrag für die Arbeitgeberattraktivität der Stadt Zofingen.

Der Schwerpunkt der Umsetzung liegt bei der Verwaltung im engeren Sinn. Die Arbeitsplätze der Schule sind bereits auf einem neueren Stand. Mit Optimierungen und Anpassungen bei Basis-Diensten wie Netzwerk, WLAN und weiteren Diensten werden Synergien mit der Schule geschaffen. Die Organisation und die Systeme der Verwaltung und der Schule werden fortlaufend und zunehmend aufeinander abgestimmt.

Die IT-Sicherheit und der Datenschutz sind bei der Umsetzung der IT-Strategie zentrale Komponenten und werden bei allen Massnahmen berücksichtigt. Neben den technischen Massnahmen werden die digitalen Kompetenzen der Anwender/-innen gezielt gefördert.

Für die Umsetzung ist ein enges Zeitfenster vorgesehen, um einerseits die Betriebssicherheit zu garantieren und anderseits möglichst eine kurze Phase des Parallelbetriebs der bisherigen und der neuen Infrastruktur zu haben. Die Umsetzung erfolgt in den Jahren 2024 bis 2025.

II Ausgangslage und Stossrichtungen

Der Stadtrat hat am 4. Mai 2022 die IT-Strategie der Stadt Zofingen verabschiedet. Die Strategie umfasst alle Bereiche der Stadt Zofingen (inkl. Schule). Gestützt darauf wurde die Umsetzung als Grundlage für den vorliegenden Antrag geplant.

1. Stossrichtungen der IT-Strategie

In der IT-Strategie wurden fünf Stossrichtungen mit ihren jeweiligen Zielen erarbeitet.

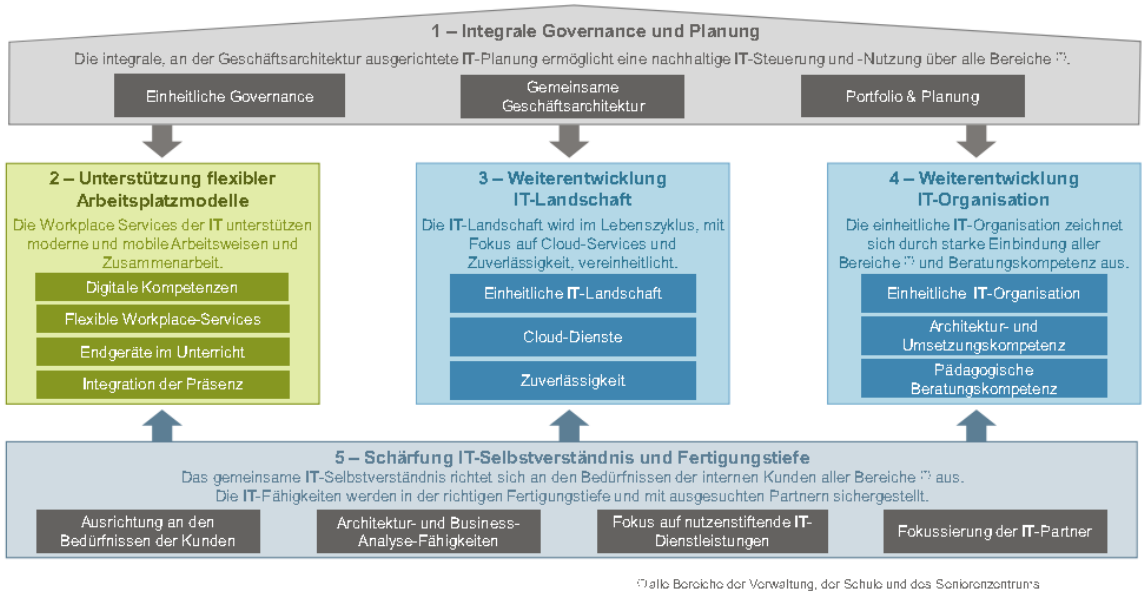

Abbildung 1: Strategiehaus mit strategischen Stossrichtungen

Der vorliegende Antrag fokussiert sich auf die Umsetzung der Stossrichtung 2 "Unterstützung flexibler Arbeitsplatzmodelle" und der Stossrichtung 3 "Weiterentwicklung IT-Landschaft". Diese zwei Stossrichtungen werden mit dem beantragten Verpflichtungskredit umgesetzt und in den nächsten zwei Kapiteln beschrieben. Die weiteren drei Stossrichtungen werden laufend und parallel dazu umgesetzt und sind in diesem Verpflichtungskredit nicht enthalten, da sie vor allem organisatorische Aspekte und das Selbstverständnis der Organisation betreffen.

1.1. Stossrichtung 2 - Unterstützung flexibler Arbeitsplatzmodelle

Mit der Stossrichtung 2 werden mit den Workplace-Services der IT die flexiblen und mobilen Arbeitsweisen und die Zusammenarbeit unterstützt. Diese Infrastruktur und Dienstleistungen sind heute Standard und Voraussetzung für ein effizientes Arbeiten und zentral für die Arbeitgeberattraktivität. Die Dienstleistungen sollen auf die spezifischen Bedürfnisse der Bereiche der Verwaltung, der Schule und des Seniorenzentrums ausgerichtet sein. Zudem sollen die digitalen Kompetenzen der Anwender/-innen gezielt gefördert werden.

Die Stossrichtung 2 beinhaltet folgende konkreten Umsetzungsziele:

- *Digitale Kompetenzen*
  Die digitalen Kompetenzen der Anwender/-innen werden durch die Personalentwicklung fachspezifisch gefördert.
- *Flexible Workplace-Services*
  Die Endgeräte und die Ausstattung der Arbeitsplätze unterstützen bedarfsgerecht die flexible und die mobile Gestaltung der Arbeitsweisen.

- *Integration der Präsenz*
  Die IT-Services unterstützen mit Plattformen und physischer Ausstattung von Räumen eine flexible Kombination von virtueller und physischer Präsenz, Kommunikation und Zusammenarbeit. Dies betrifft alle Anspruchsgruppen (Einwohner/-innen, Verwaltungsangestellte, Lehrpersonen, Schüler/-innen).

1.2. Stossrichtung 3 – Weiterentwicklung IT-Landschaft

Entlang der Stossrichtung 3 wird die IT-Landschaft im Lebenszyklus vereinheitlicht. Dabei liegt der Fokus auf der bevorzugten Nutzung von Cloud-Diensten sowie auf Zuverlässigkeit und Wirtschaftlichkeit.

Die Stossrichtung 3 beinhaltet folgende konkreten Umsetzungsziele:
- *Einheitliche IT-Landschaft*
  Die IT erbringt ihre IT-Services auf Basis einer einheitlichen und konsolidierten Landschaft von IT-Infrastrukturen und unterstützenden Services bedarfs- und kostenoptimiert.
- *Cloud-Dienste*
  Die Stadt setzt für ihre IT-Services sowie für Fachapplikationen und -plattformen bevorzugt Cloud-Dienste ein.
- *Zuverlässigkeit*
  Die Verfügbarkeit und Betriebszeiten der IT-Services werden auf die Anforderungen bezüglich Zuverlässigkeit ausgerichtet.

III IST-Situation IT-Landschaft

1. Basis-Infrastruktur Schule und Verwaltung

Die Basis-Infrastruktur der Schule und der Verwaltung sind voneinander getrennt und funktionieren eigenständig. Das Netzwerk, das WLAN und die Druckerservices der Schule und der Verwaltung werden getrennt und eigenständig betrieben. Bei der Telefonie setzt die Verwaltung (exkl. Seniorenzentrum) das 3CX-Kommunikationssystem ein. Die Schule hat pro Schulstandort eine eigenständige Anbindung ans Telefonnetz.

2. IT-Umgebung Verwaltung

Die IT-Umgebung der Verwaltung umfasst rund 280 Benutzer/-innen. Einzelne Benutzer/-innen teilen sich eine Arbeitsstation. Die ca. 235 Arbeitsplätze der Verwaltung werden als virtuelle Clients betrieben. Der grösste Teil der Mitarbeitenden haben als Arbeitsplatz ein reines Terminal (ca. 184 Arbeitsplätze), auf dem der virtuelle Client gestartet wird. Die Terminals wurden 2013 beschafft. Eine Minderheit der Arbeitsplätze (ca. 51 Arbeitsplätze) ist mit einem Notebook ausgestattet.

Die virtuellen Clients haben als Betriebssystem Windows 10 Enterprise. Die offizielle Unterstützung von Windows durch Microsoft endet im Oktober 2025. Spätestens auf diesen Zeitpunkt müssten die virtuellen Clients neu konfiguriert werden. Bei den Office-Programmen wird die Version Office2016 eingesetzt. Die offizielle Unterstützung von Microsoft endet am 14.10.2023. Mit dem Ende der Unterstützung werden auch Zugriffe auf einzelne Webdienste von Office365 aus den Office2016-Applikationen nicht mehr verfügbar sein. Ein Update auf eine neuere Version der Office-Applikationen ist zwingend.

Die Server-Umgebung für den Betrieb der virtuellen Clients der Applikationen wird vor Ort betrieben. Die Server-Umgebung wurde im Jahr 2016 beschafft und 2017 in Betrieb genommen. Sie umfasst 32 Server, davon dienen 20 Server dem Betrieb der virtuellen Clients und 12 Server dem Betrieb der Applikationen. Aktuell sind 84 Applikationen im Einsatz, davon werden bereits 21 als Cloud-Lösungen betrieben.

3. IT-Umgebung Schule

Die IT-Umgebung der Schule beinhalt die Arbeitsplätze der Lehrpersonen, Schulleitungen und aller Schülerinnen und Schüler. Die Arbeitsplätze der Schulverwaltung werden durch die IT der Verwaltung zu Verfügung gestellt. Als Endgeräte stehen im Schulnetzwerk aktuell 390 Desktop-PCs bzw. Notebooks sowie 1'490 Tablets im Einsatz. Sämtliche Lehrpersonen und alle Schülerinnen und Schüler ab der 5. Klasse sind mit einem personalisierten Tablet ausgerüstet. Bis zur 5. Klasse stehen Poolgeräte zur Verfügung. Alle Geräte sind von Apple und werden mit OSX respektive iOS betrieben.

Sämtliche rund 1'750 Benutzer (Lehrpersonen, Schulleitung und Schülerinnen und Schüler) werden in der Software CMI Lehreroffice erfasst und verwaltet. Anhand der dort zugeteilten Klassen werden automatisch die Rollen und Benutzerrechte für den Zugriff auf Dateiablagen und Applikationen vergeben. Die Bereitstellung der Geräte wird automatisiert anhand den Rollen und Rechte des jeweiligen Benutzers durchgeführt.

Das Zusammenspiel der administrativen Software CMI Lehreroffice mit den technischen IT-Systemen wie Jamf, Microsoft Azure, Apple School Manger und Office365 ist perfektioniert und für die Bedürfnisse der Schule optimiert. Der grösste Teil der Server-Dienste ist bereits in die Cloud der jeweiligen Anbieter verlagert.

Die Netzwerke (LAN und WLAN), Drucker und die Telefonie sind getrennt von der Infrastruktur der Stadtverwaltung.

IV Umsetzung – Zielbild

Für die Umsetzung leitet sich aus der IT-Strategie folgendes Zielbild ab:

- Alle Mitarbeitenden der Stadt Zofingen (Schule und Verwaltung) nutzen eine bedarfsorientierte technische Infrastruktur, welche mobiles Arbeiten ermöglicht.
- Eine gemeinsame Netzwerk-Infrastruktur (LAN + WLAN) ermöglicht das Arbeiten an jedem Standort der Schule und Verwaltung.
- Alle Mitarbeitenden sind über eine einheitliche Telefonielösung erreichbar.
- Ein Follow-Me Printing-Service ist für alle Mitarbeitenden an allen Standorten vorhanden.
- Für das kollaborative Arbeiten mit internen und externen Partnern werden geeignete Mittel zur Verfügung gestellt.
- Die Datensicherheit und der Datenschutz sind jederzeit gewährleistet.
- Nebst der Datenablage in den Fachapplikationen und der Geschäftsverwaltungslösung kann auf gemeinsame Ablagestrukturen zugegriffen werden.
- Die digitalen Werkzeuge ermöglichen bereichs- und abteilungsübergreifende, teilweise auch automatisierte Prozesse.

- Die Mitarbeitenden sind befähigt, mit den neuen Mitteln zu arbeiten.
- Die Bedürfnisse der Bereiche und Abteilungen werden konsequent umgesetzt.

Zur Umsetzung werden drei Bereiche definiert:
- Basisdienste
- Digital Workplace
- Office365

Dabei werden Basisdienste für die Schule und die Verwaltung gemeinsam betrieben und weiterentwickelt. Die spezifischen Dienste der Schule und der Verwaltung wie die jeweiligen Fachapplikationen, der Digital Workplace (Clients und Server), die Rollen- und Rechteverwaltung und die Office365-Umgebung werden weiterhin spezifisch für Schule und Verwaltung sichergestellt. Dort wo Synergien möglich sind, werden diese genutzt. Die Leitung der Informatik und die Koordination der einzelnen Themen erfolgt gemäss Stossrichtung 4 einheitlich und gemeinsam.

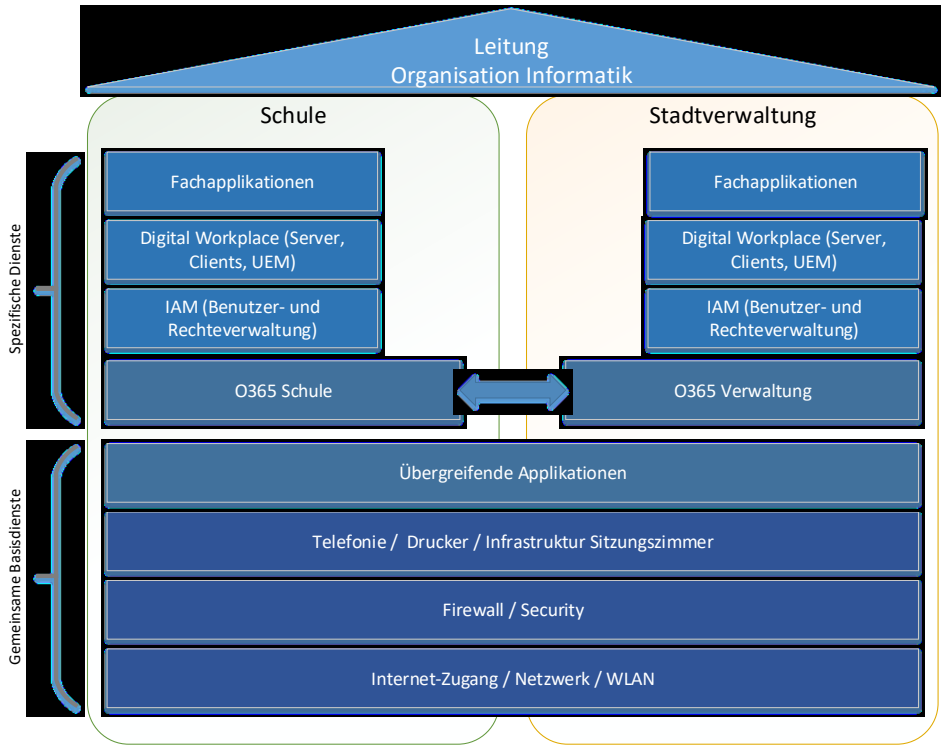

Abbildung 2: Aufteilung gemeinsame Basisdienste und spezifische Dienste Schule und Stadtverwaltung

Der vorliegende Antrag umfasst die gemeinsamen Basisdienste der Schule und der Stadtverwaltung sowie die spezifischen Dienste der Stadtverwaltung. Die spezifischen Dienste der Schule sind nicht Bestandteil des Antrages.

1. Basisdienste

Die Basisdienste Netzwerk, WLAN, Firewall, Cyber-Security, Telefonie, Druckerdienste, Infrastruktur der Sitzungszimmer und übergreifende Applikationen wie CMI werden zusammengeführt und fortlaufend vereinheitlicht. Durch die Zusammenlegung wird die übergreifende Zusammenarbeit vereinfacht.

Folgende Themenbereiche werden im Umsetzungsprojekt im Detail erarbeitet und umgesetzt. Die Abschätzung der Kosten sind in der Kostenaufstellung unter der Position Projekte Infrastruktur aufgeführt:

- Zusammenfassung Netzwerk-Infrastruktur
- Erneuerung WLAN-Verwaltung
- Optimierung Telefonie
- Optimierung Printerservices
- Infrastruktur Sitzungszimmer
- Aufbau einheitlicher Helpdesk

2. Digital Workplace

Die Ausführungen zum Digitalen Workplace fokussieren sich auf die Stadtverwaltung. Das Client-Konzept der Schule wurde während der Erarbeitung der Umsetzungsplanung der IT-Strategie detailliert analysiert. Mit dem vorhanden Client-Konzept kann die Schule aktuell optimal alle Bedürfnisse der Lehrpersonen und der Schüler/-innen abdecken. Das Design der Benutzer- und Geräteverwaltung der Schule entspricht dem Zielbild des Konzepts für die Stadtverwaltung. Synergien werden, wo vorhanden, in der Umsetzung berücksichtigt.

2.1. Mobile Geräte

Die bestehenden Terminals werden durchgängig mit Notebooks ersetzt. Die Applikationen werden direkt auf dem Notebook installiert oder über die Cloud bezogen. Dies ermöglicht das mobile Arbeiten für alle Mitarbeitenden mit einem PC-Arbeitsplatz. Desk-Sharing, Arbeiten in Sitzungszimmern und unterwegs sowie Home-Office werden technisch ermöglicht. Aktuell müssen Mitarbeitende mit Terminals ihre private Infrastruktur für das Home-Office zur Verfügung stellen.

Die Geräte und Benutzer werden zentral mit Microsoft Intune verwaltet, damit können sämtliche Belange des Gerätes zentral verwaltet werden (Betriebssystem und Updates, Endpoint-Security, Netzwerk, Benutzer, Zugriffsberechtigungen, Applikationen).

Ein Arbeitsplatz besteht nebst dem Notebook aus zwei Monitoren (oder einem grossen Monitor), Tastatur, Maus und Headset. Es stehen verschiedene Gerätekategorien zur Verfügung:

- Standard Notebook für Normalanwender/-innen
- Leichtes kleineres Notebook für Mitarbeitende, welche häufig unterwegs sind
- Notebook mit höherer Leistung für Arbeitsplätze mit grafischen Anwendungen für CAD-Daten und Grafik-Daten

Bei Teilzeitpensen unter 20 % wird auf ein persönliches Gerät verzichtet, und es wird ein Abteilungsgerät zur Verfügung gestellt. Die Verwendung von privaten Geräten (Bring Your Own Device) ist nicht vorgesehen.

Die genauen Spezifikationen werden im Rahmen der Ausschreibung erarbeitet. Die Kosten in der Kostenübersicht sind mit einem Mittelwert aus handelsüblichen Geräten berechnet.

2.2. Fachapplikationen und Server-Dienste

Die lokalen Server-Dienste und die aktuell lokal betriebenen Fachapplikationen werden alle in die Cloud verlagert. Dort wo möglich, wird die Software direkt als Dienstleistung beim Hersteller als SaaS- (Software as a Service) oder Web-Lösung bezogen. Bereits umgesetzte Beispiele für SaaS-Lösungen sind die Geschäftsverwaltungslösung CMI oder die Zeiterfassungs-Software Click Time.

Bei Softwarelösungen welche nicht durch den Lösungsanbieter in der Cloud bezogen werden können, werden die aktuell lokal betriebenen Server in die Azure-Cloud von Microsoft verschoben.

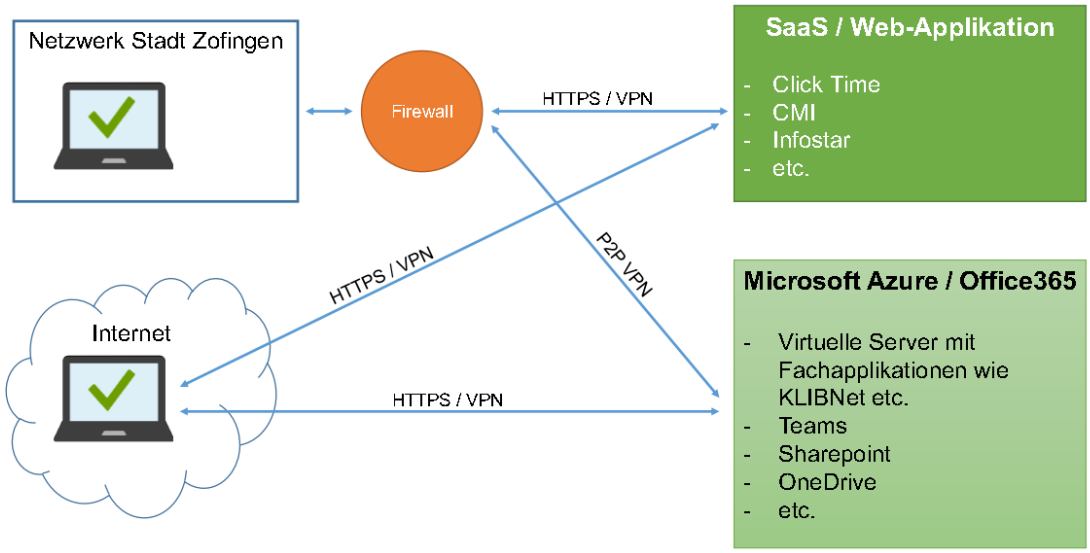

Abbildung 3: Vereinfachte schematische Darstellung des Zugriffs auf die Cloud-Dienste

2.3. Dateiablagen

Die klassischen bestehenden Dateiablagen wie Abteilungslaufwerke werden durch folgende Struktur abgelöst:

- Datenablage in Fachapplikationen, z. B. Fallführung Bereich Soziales in Fachapplikation KLIBNet.
- Geschäftsführung in Geschäftsverwaltungslösung CMI
- Ablage von nicht geschäftsrelevante Daten in Microsoft Teams und Sharepoint
- Ablage von persönlichen Arbeitsdaten auf Microsoft OneDrive

Die Zuweisung der Daten auf die jeweilige Datenablage wird im Datenkonzept geregelt. Die Einhaltung der Vorgaben des Datenschutzes ist zwingend, besonders beim Speichern und Bearbeiten von Personendaten und besonders schützenswerten Personendaten.

2.4. IAM Zugriffskonzept

Für den sicheren und geregelten Zugriff der Mitarbeitenden auf die ihnen zugeteilten IT-Ressourcen wird ein Identity + Access Management (IAM) eingeführt. Die Basis für das IAM bildet das Rollen- und Rechtekonzept. Das Rechte- und Rollenkonzept legt die einzelnen Rollen (Funktionen und Tätigkeiten) in den Bereichen fest und definiert die dazugehörigen Rechte der einzelnen Rollen, d. h. welche Applikation darf mit welchen Berechtigungen verwendet werden, auf welche Daten darf mit welchen Rechten zugegriffen werden.

Mittels IAM wird bei einem Zugriff auf die IT-Systeme zuerst die Identität (Rolle) einheitlich geprüft und im Anschluss werden der Identität (Rolle) die zugehörigen Rechte vergeben. Der Anmelde-prozess für die Anwender/-innen wird vereinfacht, und das mehrfache Anmelden und Authen-tifizieren entfällt weitestgehend (Single Sign On).

2.5. IT-Sicherheit Zero-Trust Konzept

Die IT-Sicherheit wird anhand des Zero-Trust Konzept aufgebaut. Das Konzept basiert auf drei Standbeinen:

1. Explizite Kontrolle nach dem Schema von aussen gegen innen:
   - Prüfung der Identität
   - Prüfung des Standorts
   - Prüfung des Endpoints (Gerät)
   - Prüfung des Zugriffs auf eine Applikation
   - Prüfung des Netzwerks
   - Prüfung der Infrastruktur (Server, Dateiablagen)
   - Prüfung der Datenklassifizierung
2. Geringstmögliche Berechtigung:
   - Risikobasierte Vergabe von Berechtigungen
   - Nur notwendige Berechtigungen
   - Berechtigungen zeitlich nur dann, wenn sie benötigt werden
3. "Was tun wenn"-Szenarien
   - Automatiserte Erkennung und Abwehr von Bedrohungen
   - Minimieren der Ausbreitung in Schadenszenarien

Die konsequente einheitliche Verwaltung der Clients mittels Windows Intune und die Virtualisierung der Server in der Microsoft Azure Cloud ermöglicht den Einsatz eines einheitlichen IT-Security-Konzepts, basierend auf Windows Defender. Die Pflege der IT-Sicherheitsrichtlinien und die Überwachung durch die Informatik wird dadurch stark vereinfacht.

Das sichere Login-Verfahren für den Mitarbeitenden wird durch die Mehrfach-Authentifizierung mittels Microsoft Authenticator auf allen Geräteklassen (Notebooks, Tablets, Smartphones) sichergestellt. Die Mehrfach-Authentifizierung mittels Microsoft Authenticator ist bereits bei der Anmeldung der heutigen virtuellen Clients im Einsatz.

3. Office365

Der Wechsel auf eine neue Generation der Office-Applikationen ist duch das End-Of-Life der aktuellen Office2016-Applikationen per 14.10.2023 ein Muss.

Die Office365-Umgebung bietet nebst den klassischen Anwendungen wie Word, Excel und PowerPoint eine Vielzahl von zusätzlichen Applikationen zur persönlichen Arbeitsorganisation und zur Zusammenarbeit. Die Zusammenarbeit über Bereichs- und Abteilungsgrenzen hinweg und mit externen Partnern wird vereinfacht und erleichtert. Die Verwendung der neuen Kommunikationsmöglichkeiten Video-Konferenz und Teams-Chat wird im Kommunikationskonzept geregelt. Die Festnetz-Telefonie mittels Teams ist aktuell nicht vorgesehen, wird aber bei Erarbeiten der Optimierungsmassnahmen Telefonie miteinbezogen. Der Zugriff auf die Applikationen und die Dateiablagen ist jederzeit mittels Notebook, Tablets und Smartphone möglich.

Die Konfiguration der Office365-Umgebung und die Festlegung der Regelungen wie z. B. das Teilen von Daten oder die Verwendung von Applikationen sind im Office365-Konzept beschrieben und geregelt. Das Office365-Konzept wurde während der Projektphase "Planung der Umsetzung der IT-Strategie" erstellt.

3.1 Zusatzdienste innerhalb Office365

Folgende Zusatzdienste werden für die Office365 Umgebung angepasst oder neu aufgebaut:

- *Vorlagenmanagement mittels Office At Work*
  Die bestehende Vorlagenmanagement-Lösung Office At Work wird aktualisiert und die bestehenden Vorlagen werden angepasst.
- *Intranet*
  Auf der Basis von SharePoint und Microsoft Teams wird mit einer Softwareerweiterung für die Mitarbeitenden ein Intranet aufgebaut. Die Office365-Umgebung wird für den Mitarbeitenden dadurch der zentrale Ort, um Zugriff auf alle relevanten Informationen zu haben.
- *Automatisierungen für Microsoft Teams*
  Zur einfacheren und standardisierten Erstellung von Microsoft-Teams Teams und Kanälen wird eine Erweiterung eingesetzt, mit der man auf Grund von Vorlagen in einfachen Schritten neue Teams und Kanäle anlegen kann, z. B. für Projekte.
- *Prozessmanagement*
  Die bestehende Lösung der Prozessdokumentation wird abgelöst durch eine einfache für alle Mitarbeitende verfügbare Dateiablage innerhalb von SharePoint und Teams. Sie wird mit dem Intranet verknüpft.

V Umgang mit Cloud-Diensten

Die Verlagerung von IT-Ressourcen zu Clouddienstleistern führt dazu, dass folgende Themen besonders beachtet werden müssen:

- Datenschutz
- IT-Sicherheit
- Verfügbarkeit der IT-Ressourcen
- Abhängigkeit von Lieferanten

1. Datenschutz

Die Stadt Zofingen und die ihr angegliederten Organisationen unterstehen folgenden Gesetzgebungen im Bereich des Datenschutzes:

- Bundesgesetz über den Datenschutz (DSG; SR 235.1)
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11)
- Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau (IDAG; SAR 150.700)
- Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau (SAR 150.711).

Die Verlagerung von Daten zu Clouddienstleistern ist unter Einhaltung der Vorgaben von Verschlüsselungen aus datenschutzrechtlicher Sicht machbar. Die Bundesverwaltung, kantonale Verwaltungen und diverse kommunale Verwaltungen haben in den letzten Jahren unter Einhaltung der Vorgaben Verlagerungen durchgeführt. Bei Verlagerung von Daten auf Clouddienste müssen die Aspekte des Datenschutzes besonders beachtet werden. Nebst der Erstellung des Datenkonzepts und des Datenschutzkonzepts wird vor der Einführung eine Datenschutzfolgeabklärung erstellt und durch die kantonale Behörde (Beauftragte für Öffentlichkeit und Datenschutz ÖDB) geprüft.

2. IT-Sicherheit

Der Schutz der Daten vor missbräuchlichem Zugriff hat höchste Priorität. Die Umsetzung des Zero-Trust-Prinzips mit Einbezug der Clouddienste schafft eine deutliche höhere Sicherheit, als wenn man alle IT-Sicherheitsmassnahmen auf einer lokalen Infrastruktur betreibt. Die Clouddienstleister können innert kürzester Zeit auf die aktuellen Bedrohungslagen reagieren und haben wesentlich grössere Ressourcen und Fachspezialisten im Bereich der IT-Sicherheit als eine interne IT-Organisation.

3. Verfügbarkeit der IT-Ressourcen

Bereits heute sind die meisten Dienste abhängig vom Internet und der Cloud, so zum Beispiel die Kommunikation mittels Email oder die Mehrfach-Authentifizierung bei der Anmeldung am PC.

Cloud-Dienstleister können im Vergleich zu einem lokal betriebenen Rechenzentrum insgesamt eine bessere Verfügbarkeit und Sicherheit ihrer Dienste garantieren. Nur mit sehr hohem Aufwand sind bei einer lokalen Infrastruktur die gleichen Standards wie in einem Tier IV zertifizierten Rechenzentrum zu erreichen.

Bei einem Stromausfall ist ein lokales Rechenzentrum nur für eine beschränkte Zeit noch verfügbar, da die unterbrechungsfreie Stromversorgung (USV) nur für das geordnete Sichern der Daten und das Runterfahren der Systeme ausgelegt ist. Die Netzwerkinfrastruktur an den verschiedenen Standorten der Stadtverwaltung ist bei einem Stromausfall sofort nicht mehr verfügbar und damit sind auch die lokalen Serversysteme nicht mehr erreichbar.

Bei einem lokal beschränkten Stromausfall können alle Cloud-Dienste weiterhin von anderen Standorten aus bezogen werden. Durch die Verwendung von mobilen Arbeitsgeräten kann so z. B. aus dem Home-Office bei vorhandener Internet-Verbindung auf die Dienste zugegriffen werden.

Der Zugriff auf Daten, welche bei grossräumigen Ausfallszenarien zur Verfügung stehen müssen, muss besonders geregelt werden. Es handelt sich hier um Daten aus den Bereichen Feuerwehr und Bevölkerungsschutz, der Regionalpolizei aber auch um Daten der Einwohnerkontrolle.

Eine regelmässige Synchronisation der Daten auf lokale Notfallsysteme ist eine Möglichkeit zur Sicherstellung der Datenverfügbarkeit. Solche Notfallsysteme können im Gebäude der Stützpunktfeuerwehr Zofingen betrieben werden, da dieses Gebäude über einen Notstromgenerator mit Strom versorgt werden kann.

Die Beurteilung der Risiken, die Ausfall- und Wiederherstellzeiten und die Sicherheitsmassnahmen werden im IT-Sicherheitskonzept beschrieben.

4. Abhängigkeit von Lieferanten

Die bereits bestehende grosse Abhängigkeit zu wichtigen Herstellern und Lieferanten von Software-Produkten, wie z. B. Microsoft wird durch die Verlagerung von Diensten in die Cloud nochmals grösser. Dieser Abhängigkeit kann durch Standardisierung der Virtualisierungs-Technologie teilweise entgegengewirkt werden. Die Standardisierung ermöglicht bei den Server-Diensten den Rechenzentrum-Anbieter zu wechseln.

VI Schulung

Die geplante Umstellung auf den neuen Digital Workplace und auf die Office365-Umgebung stellt einen grossen Umbruch für alle Mitarbeitenden dar. Die bedarfsgerechte Ausbildung ist ein wesentlicher Faktor für eine erfolgreiche Umsetzung. Die Schulung der digitalen Fähigkeiten ist umso wichtiger, weil diese in der Vergangenheit vernachlässigt wurde.

Parallel zum Aufbau der technischen Systeme werden die Schulungsunterlagen und Schulungskonzepte erarbeitet. Es ist vorgesehen, die Schulungen gemeinsam mit einem externen Partner durchzuführen, welcher auf die Schulung von Office365 spezialisiert ist.

1. Ausbildung Mitarbeitende Informatik

Der wesentliche Teil der Ausbildung der IT-Mitarbeitenden findet während der Projektumsetzung statt. Die Umsetzungspartner richten gemeinsam mit den IT-Mitarbeitenden die Systeme ein und erstellen die technischen Dokumentationen. Nebst dieser Art von Wissensaufbau müssen die IT-Mitarbeitenden für spezifische Themen gezielt befähigt werden. Bei den Projektkosten sind Schulungen im Umfang von insgesamt 65 Stunden vorgesehen.

2. Ausbildung Anwender/-innen

Die Schulungen der Mitarbeitenden werden bedarfsgerecht und auf den Arbeitsalltag bezogen durchgeführt. Pro Bereich oder Abteilung gibt es einen oder mehrere IT-Poweruser, welche im Projekt mitarbeiten und als Test-Anwender/-innen in der Phase des Proof Of Concept die bereichs- und abbteilungsspezifischen Prozesse testen. Die Poweruser sind bei der Umstellung die erste Anlaufstelle für die Anwender/-innen.

VII Kostenübersicht

1. Investitionskosten für die Umsetzung der IT-Strategie

Arbeitsplätze Mitarbeitende	Kosten / Stück (CHF)	Anzahl	Kosten (CHF)
Notebooks	1'200	250	300'000
Peripherie (Monitore, Dockingstation)	775	250	193'750
Summe			**493'750**

Projektaufwand	Kosten / Projekttag	Anz. Tage	Kosten (CHF)
Projektkosten O365	1'520	24	36'480
Projektkosten Digital Workplace	1'680	48	80'640
Projektkosten Anpassungen Netzwerk	1'680	5	8'400
Projektkosten Einführung IAM	1'680	10	16'800
Projektkosten IT-Security	1'680	10	16'800
Summe			**159'120**

Software Lizenzen einmalig	Kosten / Stück (CHF)	Anzahl	Kosten (CHF)
Intranet-Erweiterung für SharePoint	15'000	1	15'000
Automatisierungen für Microsoft Teams	3'000	1	3'000
Erneuerung Vorlagenmanagement für Office365	22'000	1	22'000
Erweiterung Prozessmanagement	16'000	1	16'000
Summe			**56'000**

Software Lizenzen wiederkehrend (Erstbeschaffung)	Kosten / Stück pro Jahr (CHF)	Anzahl	Kosten (CHF)
MS E5 inklusive Windows	720	250	180'000
MS Mail-Lizenz für User ohne IT-Arbeitsplatz	48	300	14'400
Lizenzen Azure-Services (Server + Dienste)	48'000	1	48'000
Lizenzen Backup-Dienste	5'000	1	5'000
Lizenzen Mail-Archiv	12	450	5'400
Lizenzen IAM	48	450	21'600
Lizenzen Prozessmanagement	5'000	1	5'000
Lizenzen Intranet	3'000	1	3'000
Lizenzen Vorlagenmanagement	5'000	1	5'000
Summe			**287'400**

Projekte Basisdienste	Projektkosten (CHF)	Anzahl	Kosten (CHF)
Infrastruktur Sitzungszimmer	50'000	1	50'000
Zusammenfassung Netzwerk-Infrastruktur	20'000	1	20'000
Erneuerung WLAN Verwaltung	25'000	1	25'000
Optimierung Telefonie	10'000	1	10'000
Optimierung Printservices	10'000	1	10'000
Aufbau einheitlicher Helpdesk	10'000	1	10'000
Summe			**125'000**

Schulung	Kosten / Schulungsstd. (CHF)	Anzahl	Kosten (CHF)
Schulung Mitarbeitende IT	190	65	12'350
Schulung Benutzer	190	250	47'500
Summe			**59'850**

Reserve und Rundung	Kosten (CHF)
Summe	**53'880**

Gesamtkosten	1'235'000

Die Beschaffung der Hardware (Pos. 1 Arbeitsplätze Mitarbeitende) muss öffentlich ausgeschrieben werden. Die Beschaffung der Software-Lizenzen kann freihändig erfolgen, da die einmaligen Kosten den Schwellwert für eine öffentliche Beschaffung nicht erreichen und die wiederkehrenden Kosten eine Erweiterung der bestehenden Lizenzen sind.

Die Kosten des Projektaufwands basieren auf den Schätzungen möglicher Partner für die Umsetzung der jeweiligen Themen. Die Schätzungen wurden bei der Erarbeitung des Konzepts ermittelt.

2. Abschreibungen und Folgekosten

Die beschaffenen Geräte, Software, Projektkosten und Schulungsaufwand werden über einen Zeitraum von drei Jahren ab dem Folgejahr der Inbetriebnahme linear abgeschrieben. Folglich erhöhen sich die Abschreibungen zu Lasten der Erfolgsrechnung im Zeitraum 2025 bis 2027 um jährlich brutto CHF 370'000.

Die Projekte Basisdienste werden im Durchschnitt über einen Zeitraum von drei Jahren ab dem Folgejahr der Inbetriebnahme linear abgeschrieben. Folglich erhöhen sich die Abschreibungen zu Lasten der Erfolgsrechnung im Zeitraum 2025 bis 2027 um jährlich CHF 41'666.

Im Jahr 2028 ist vorgesehen, die Arbeitsgeräte zu ersetzen, die Investitionen von CHF 650'000 sind im Finanz- und Investitionsplan berücksichtigt (1.0222.5060.00 /Ersatzbeschaffung IT-Hardware nach Lebensdauer).

3. Software-Wartungskosten

Die wiederkehrenden Software-Lizenzen werden im Beschaffungsjahr als Investition ausgewiesen. Im Folgejahr der Investition werden die Kosten im Budget unter Informatik/Unterhalt Software Kto. 1.0222.3158.00 verbucht.

Die jährlichen Software-Wartungskosten erhöhen sich insgesamt von heute CHF 102'853 um CHF 179'747 auf CHF 282'600. Der Mehrkosten werden vorwiegend durch die Microsoft-Lizenzen verursacht.

Software Lizenzen wiederkehrend	**Kosten neu (CHF)**	**Kosten Ist (CHF)**	**Mehrkosten (CHF)**	**Bemerkung**
MS E5 inklusive Windows	180'000	11'000	169'000	Ist: Exchange Online
MS Mail-Lizenz für User ohne IT-Arbeitsplatz	9'600	-	9'600	Neu
Lizenzen Azure-Services (Server + Dienste)	48'000	72'553	-24'553	Ist: Microsoft, VMWare, Dell, Barracuda, Nutanix, Nextcloud
Lizenzen Backup-Dienste	5'000	4800	200	Ist: Veeam
Lizenzen Mail-Archiv	5'400	-	5'400	Neu
Lizenzen IAM	21'600	-	21'600	Neu
Lizenzen Prozessmanagement	5'000	10'000	-5'000	Ist: Publis
Lizenzen Intranet	3'000	-	3'000	Neu
Lizenzen Vorlagenmanagement	5'000	4'500	500	Ist: Office at Work
Summe	**282'600**	**102'853**	**179'747**	

4. Minderaufwand durch Wegfall der Server-Infrastruktur

Die Umsetzung der IT-Strategie führt wie oben dargelegt zu einem jährlich wiederkehrenden Mehraufwand durch die Abschreibungen (ca. CHF 412'000) und Lizenzen (ca. CHF 180'000).

Im Gegenzug reduziert sich der Beschaffungs- und Unterhaltsaufwand für die Server in der Erfolgsrechnung um jährlich durchschnittlich ca. CHF 200'000. Der wiederkehrende Nettomehraufwand beträgt somit ca. CHF 392'000, wobei dieser sich nach drei Jahren (Wegfall Abschreibung Projekte Basisdienste) auf ca. CHF 350'000 reduziert wird.

5. Gegenüberstellen mit dem 1:1-Ersatz der bestehenden Infrastruktur und Arbeitsplätze

Auch ohne die Umsetzung der formulieren Strategie, müsste die bestehende Infrastruktur komplett erneuert werden. Der Aufwand für den Ersatz der Server-Infrastruktur vor Ort, der Terminals mit virtuellem Desktop und der Wechsel der Office Version werden Investitionskosten in der Grössenordnung von CHF 920'000 erwartet. Die Ausstattung der Arbeitsplätze mit Laptops, die Einführung der Clouddienste und der Wechsel der Office Version gemäss der Strategie sind im vorliegenden Kredit

mit einem vergleichbaren Aufwand (ca. CHF 900'000) abgebildet. Eine komplette Erneuerung der bestehenden Infrastruktur wäre somit nicht günstiger und würde deutliche weniger zu einer modernen und mobilen Arbeitsweise beitragen. Weitere CHF 50'000 aus dem Verpflichtungskredit tragen zur Harmonisierung der zwischen der Schul- und der Verwaltungsinformatik bei, was in Zukunft die Nutzung von Synergien ermöglicht.

Die verbleibenden rund CHF 280'000 ergeben sich vorwiegend aus der Konzeptarbeit (Projektkosten), der Einführung des Intranets, den zusätzlichen Mails, so dass alle Mitarbeiter/-innen elektronisch erreichbar sind, sowie aus der Optimierung des WLANs und der digitalen Ausrüstung der Sitzungszimmer.

VIII Termine

Thema	Q2/23	Q3/23	Q4/23	Q1/24	Q2/24	Q3/24	Q4/24	Q1/25	Q2/25	Q3/25	Q4/25
Erarbeitung O365-Konzept (erledigt)											
Erarbeitung Datenkonzept											
Detailanalyse Druckerservices											
Detailanalyse Telefonie											
Erarbeitung Datenschutzkonzept											
Technisches Konzept Clientverwaltung											
Technisches Konzept Server Microsoft Azure											
Erarbeitung Rollen- und Rechtekonzept											
Erarbeitung Kommunikationskonzept											
Aufbau Server in Microsoft Azure											
Aufbau Clientverwaltung Microsoft Intune											
Ausbau Infrastruktur Sitzungszimmer											
Erarbeitung IT-Sicherheitskonzept											
POC Sever Microsoft Azure											
POC Clientverwaltung Microsoft Intune											
GoLive Server in Microsoft Azure											
Rollout Clients											
Umstellung auf O365											
Umstellung Vorlagenmanagement auf O365											
Umsetzung Telefonie											
Analyse Netzwerkkonzept inkl. WLAN											
Umsetzung Netzwerkkonzept inkl. WLAN											
Umsetzung Druckerservices											
Einführung neuer Helpdesk											
Optimierungsarbeiten (Server, Clients)											

Die Umsetzung des Projektes ist über zwei Jahre geplant. Der GoLive der neuen Digital-Workplace-Struktur und damit der Rollout der Geräte bei den Mitarbeitenden und die Umstellung auf Office365 ist für das 3. Quartal 2024 geplant.

Vor dem GoLive wird für die Server-Verlagerung in die Cloud und die Client-Verwaltung je ein Proof Of Concept (POC) durchgeführt, um möglichst alle Abhängigkeiten und Schnittstellen zu testen.

Die Erarbeitung der einzelnen Konzepte ist bereits gestartet und Bestandteil des Planungsprojekts. Die Erstellung der Konzepte erfolgt losgelöst von der Umsetzung der IT-Strategie.

IX Antrag

Der Stadtrat stellt Ihnen folgenden

Antrag

Für die Umsetzung der IT-Strategie sei ein Verpflichtungskredit von brutto CHF 1'235'000 (inkl. MWST), zuzüglich allfälliger Teuerung, zu bewilligen.

Zofingen, 23. August 2023

Freundliche Grüsse

STADTRAT ZOFINGEN

Christiane Guyer
Stadtpräsidentin

Marco Salvini
Stadtschreiber

Glossar

3CX-Kommunikationssystem	Telefonie-, Chat- und Videokonferenzsystem
Active Directory (AD)	Zentrale Benutzerverwaltung in Microsoft Windows Umgebungen
Applikationen	Programme, Software
Azure	Microsoft Cloud-Dienst zur Verwaltung der Benutzer, Geräte und Server
Bring Your Own Device (BYOD)	Integration von privaten Geräten in der IT-Umgebung von Unternehmen, Verwaltungen und Schulen
CAD-Daten	Dokumente aus Architektur- und Konstruktionsprogrammen
Cloud-Dienste	Software und Programme, die durch einen externen Dienstleister betrieben werden und durch den Anwender/die Anwenderin über das Internet aufgerufen werden
Cyber-Security	Sicherheitsmassnahmen zur Schutz der Informatik vor böswilligen Angriffen
Desk-Sharing	Nutzung physischer Arbeitsplätze (Pulte) durch mehrere Mitarbeitenden ohne fixe Zuordnung der Arbeitsplätze
Digital Workplace	IT-Arbeitsplatz, bestehend aus Gerät (PC, Notebook) und Software
Endpoint	IT-Geräte in einem Netzwerk wie PC's, Smartphones und technische Geräte
Endpoint-Security	Schutzmassnahmen für IT-Geräte wie z. B. Virenschutz
Firewall	Soft- und Hardware zur Schutz des internen Netzwerkes vor unbefugten Zugriffen von aussen
Follow-Me Printing-Service	Follow Me Printing ermöglicht es den Mitarbeitenden eines Unternehmens, alle aktivierten Drucker bzw. jedes Multifunktionssystem im Büro zu nutzen. Druckaufträge werden dabei zentral in einer Druckwarteschlange festgehalten bis der Mitarbeiter zu einem Drucker geht, um seine Druck-Jobs abzuholen
Helpdesk	Portal zur Abwicklung von Anfragen der Anwender/-innen
HTTPS (Hypertext Transfer Protocol Secure)	Sicheres Kommunikationsprotokoll für das Internet
IAM (Identity an Acces Management)	Software zur Verwaltung von Identitäten (Benutzer) und der Steuerung der Zugriffe auf IT-Ressourcen
LAN (Local Area Network)	Lokales kabelgebundenes Netzwerk zur Verbindung der IT-Geräte
Managed Device	IT-Geräte, welche durch eine Organisation verwaltet werden und der Anwender nur beschränkte Möglichkeiten hat, Einstellungen auf dem IT-Gerät zu verändern
Microsoft Authenticator	Software von Microsoft zur sicheren Identifikation des Benutzers. Die Software wird bei Systemen mit Mehrfachauthentifizierung verwendet
Microsoft Intune	Software von Microsoft zur Verwaltung von IT-Geräten
Microsoft OneDrive	Dateiablagesystem von Microsoft, welches in die Cloud-Dienste von Microsoft eingebunden ist

Microsoft SharePoint	Web-Anwendung von Microsoft für den gemeinsamen Zugriff auf Dateien und Programme innerhalb einer Organisation
Microsoft Teams	Software von Microsoft zur Zusammenarbeit innerhalb einer Organisation
Office At Work	Software für das Vorlagenmanagement in den Microsoft Office Programmen
Office2016	Microsoft Programme wie Word, Excel und PowerPoint in der Version 2016, welche noch keine Cloud-Dienste beinhalten
Office365	Microsoft Programme wie Word, Excel und PowerPoint in der jeweils aktuellsten Version, welche auch Cloud-Dienste beinhaltet
P2P (Point to Point)	Netzwerkverbindung von einem spezifischen Punkt zu einem anderen spezifischen Punkt, z.B. von Firewall in Gebäude zu Rechenzentrum eines externen Dienstleisters
POC (Proof Of Concept)	Testsysteme und Installationen um vor der Inbetriebnahme neuer Systeme die Funktionalitäten praxisgerecht zu testen
SaaS (Software as a Service)	Coudbasiertes Softwarebereitstellungsmodell, bei dem der Cloud-Anbieter Cloud-Anwendungssoftware entwickelt und wartet, automatische Software-Updates bereitstellt und dem Kunden Software über das Internet zur Verfügung stellt
Server	Computerprogramm oder ein Gerät, welches Funktionalitäten, Dienstprogramme, Daten oder andere Ressourcen bereitstellt, damit andere Geräte oder Programme darauf zugreifen können
Single Sign On (SSO)	"Einmalanmeldung" des Benutzer an einen Identitätsdienst, welcher die Anmeldung des Benutzers an weitere Dienste, Programme, Dateiablagen etc. übernimmt, ohne dass sich der Benutzer jeweils zusätzlich anmelden muss
Terminal	Eingabegerät zur Eingabe und Anzeige von Daten, welches nur sehr wenig eigene Ressourcen hat
UEM (Unified Endpoint Management)	Einheitliche Verwaltung von Geräten (engl. Endpoints) der IT-Umgebung von Organisationen. Geräte sind PC's wie auch Smartphones und Tablets
USV	Unterbrechungsfreie Stromversorgung zur Überbrückung von Stromausfällen
Virtueller Client	PC-Arbeitsplatz, welcher virtuell auf einer zentralen Server-Umgebung zur Verfügung gestellt wird. Der virtuelle Client wird auf einem Terminal oder auf einem normalen PC gestartet und dargestellt
VPN (Virtual Private Network)	Netzwerkverbindung, welche von Unbeteiligten nicht einsehbar ist.
Windows 10 Enterprise	Betriebssystem von Microsoft für Unternehmen
WLAN (Wireless Local Area Network)	Drahtloses lokales Netzwerk, wird manchmal auch als Wifi bezeichnet
Workplace-Services	Arbeitsplatz-Gesamtpaket bestehend aus Hardware, Software und Cloud-Diensten