Datenschutzrechtliche Risikoanalyse

zum Betriebsmittel

Bildschirmarbeitsplatz (BAP)

bei der Stadt Fiktivia

(Dok-ID: RA201903051630)

BayLfD-Stand: 01.05.2022

1. Inhalt:

2. Status und beteiligte Personen:

Status	beteiligte Personen	Anmerkungen
Bearbeitung	Musterfrau, Klara (Federführung, Fachbereich) Mustertech, Eva (Beratung, IT) Muster, Hans (Beratung, bDSB)	

3. Zeitpunkt der nächsten routinemäßigen Überprüfung:

Zeitpunkt	Anmerkungen
01.01.24	

4. Anlagen und Verweise:

ID	Bezeichnung	Anmerkungen
1	Beschreibung Bildschirmarbeitsplatz (BAP)	Datenschutzrechtliche Beschreibung des Betriebtsmittels "Bildschirmarbeitsplatz (BAP)", Dok-ID: BM202110070840.
2	BSI-Baustein „SYS.2.1 Allgemeiner Client“	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

3	usw.	usw.
(…)	(…)	(…)

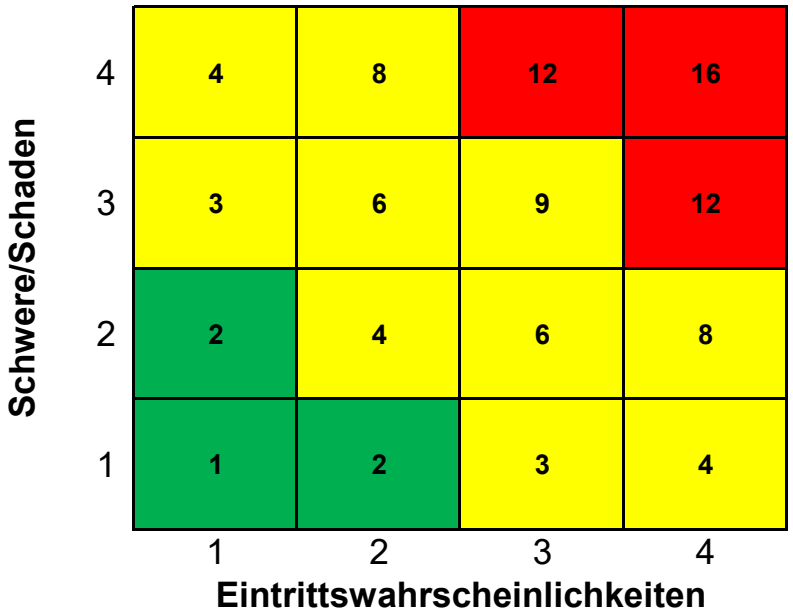
Änderungshistorie

Wann?	Wer?	Was?	Anmerkung
03.01.21	Musterfrau	Initialisierung Risikoanalyse	

Legende

1. Risikomanagement

1.1 Risikomatrix für die Indexierung der Risiken



Index	Bezeichnung Risikoindex
	hohes Risiko
	(normales) Risiko
	geringes Risiko

1.2 Eintrittswahrscheinlichkeit

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	Beispiel
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

1.3 Schwere/Schaden

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	Beispiel

1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.	**immateriell:** leichte Verärgerung **materiell:** Zeitverlust **physisch:** vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	**immateriell:** geringe, aber objektiv nachweisbare psychische Beschwerden **materiell:** deutlich spürbarer Verlust an privatem Komfort **physisch:** minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	**immateriell:** schwere psychische Beschwerden **materiell:** finanzielle Schwierigkeiten **physisch:** schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	**immateriell:** dauerhafte, schwere psychische Beschwerden **materiell:** erhebliche Schulden **physisch:** dauerhafte, schwere körperliche Beschwerden

2. Zielerfüllungsmanagement

Ergebnis der Gefährdungsbewertung

Index	Bezeichnung Gefährdungsindex
	Keine Gefährdung, d.h. prognostizierte Vollerfüllung des betrachteten Ziels
	Es kann von einer kontinuierlichen Vollerfüllung des Ziels vertretbar ausgegangen werden. Gleichwohl kann eine Gefährdung des Ziels nicht ganz ausgeschlossen werden.
	Unzureichendes Schutzniveau für das betrachtete Ziel

Arbeitsplatztypen, die in der Risikoanalyse berücksichtigt sind

AP	Bezeichnung	Beschreibung
AL	Alle Bildschirmarbeitsplätze (BAP)	Alle im Folgenden aufgezählte BAP
B*	Alle Büro-BAP	Alle im Folgenden aufgezählte Büro-BAP (interne BAP)
H*	Alle Home-Office-BAP	Alle im Folgenden aufgezählte Home-Office-BAP
M*	Alle Mobil-BAP	Alle im Folgenden aufgezählte Mobile-BAP
***P**	Alle BAP Personalbereich	Alle BAP für die Personalsachbearbeitung.
***V**	Alle BAP Verwaltung	Alle BAP in der allgemeinen Verwaltung.
BV	Büro-BAP der allgemeinen Verwaltung	Der Büro-BAP in der allgemeinen Verwaltung wird unter Verwendung der vom Arbeitgeber/Dienstherr zur Verfügung gestellten Informations- und Kommunikationstechniken betrieben und besteht aus einem Bildschirmarbeitsplatz, der einem städtischen Beschäftigten zugordnet ist und der regelmäßig insbesondere über einen Rechner (mobiler Laptop oder fester PC), ein Telefon, ein absperrbares Aktenaufbewahrungsbehältnis und Ablageflächen verfügt.
HV	Home-Office-BAP der allgemeinen Verwaltung	Der Home-Office-BAP in der allgemeinen Verwaltung wird unter Verwendung der vom Arbeitgeber/Dienstherr zur Verfügung gestellten Informations- und Kommunikationstechniken betrieben und besteht aus einem Bildschirmarbeitsplatz, der im Privatbereich des Beschäftigten genutzt wird und der regelmäßig insbesondere über einen Rechner (mobiler Laptop oder fester PC), ein Telefon, ein absperrbares Aktenaufbewahrungsbehältnis und Ablageflächen verfügt.
MV	Mobil-BAP der allgemeinen Verwaltung	Der Mobile-BAP in der allgemeinen Verwaltung wird unter Verwendung der vom Arbeitgeber/Dienstherr zur Verfügung gestellten Informations- und Kommunikationstechniken betrieben und besteht aus einem Bildschirmarbeitsplatz, der ortsungebunden vom Beschäftigen genutzt wird (z.B. Dienstreise, Dienstgang, sonstige Vor-Ort-Termine) und der regelmäßig insbesondere über einen mobilen Laptop und ein Telefon verfügt.
BP	Büro-BAP für Personalsachbearbeitung	Der Büro-BAP für Personalsachbearbeitung wird unter Verwendung der vom Arbeitgeber/Dienstherr zur Verfügung gestellten Informations- und Kommunikationstechniken betrieben und besteht aus einem Bildschirmarbeitsplatz, der einem städtischen Beschäftigten zugordnet ist und der regelmäßig insbesondere über einen Rechner (mobiler Laptop oder fester PC), ein Telefon, mehrere absperrbaren Aktenaufbewahrungsbehältnisse und Ablageflächen verfügt.
HP	Home-Office-BAP für Personalsachbearbeitung	Der Home-Office-BAP für Personalsachbearbeitung wird unter Verwendung der vom Arbeitgeber/Dienstherr zur Verfügung gestellten Informations- und Kommunikationstechniken betrieben und besteht aus einem Bildschirmarbeitsplatz, der im Privatbereich des Beschäftigten genutzt wird und der regelmäßig insbesondere über einen Rechner (mobiler Laptop oder fester PC), ein Telefon, ein absperrbares Aktenaufbewahrungsbehältnis und Ablageflächen verfügt.
usw.	usw.	
...	...	

Risikomanagement

Gewährleistungsziele	Summarische Risikobetrachtung	Index
DI - Datenintegrität VB - Verfügbarkeit VT- Vertraulichkeit	**Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.**	ge

ID	AP	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
Ziel					Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
1 VB VT	AL	**Datenverlust** Beim Einsatz von IT-Systemen können elektronische Daten verloren gehen.	# IT-Fehlfunktion # IT-User # Personal # Straftäter	Durch eine IT-Fehlfunktion (Hard- und/oder Softwarefehler, Stromausfall), eine Fehlbedienung eines IT-User (z.B. Datenüberschreibung), Geräteverlust (z.B. Liegenlassen, Diebstahl) oder einen kriminellen Angriff gehen elektronische Daten, die am BAP verarbeitet werden, unerwünscht verloren.	Nach den bisher gemachten Erfahrungen sind derartige Datenverluste nicht wahrscheinlich, da Daten, deren Verlust subtanzielle oder große Folgen haben würde, nicht auf dem IT-Arbeitsplatzrechner selbst , sondern in zentral betriebenen IT-Fachverfahren und IT-Systemen originär gespeichert werden.	1	An diversen BAP werden besonders schützenswerte elektronische Daten verarbeitet, deren Verlust mit schwerwiegenden Folgen verbunden sein könnten.	4	4	M.1 Anweisung zur Speicherung von Daten einhalten M.2 Anti-Schadsoftware-Schutz verwenden M.3 Beschäftigte sensibilisieren M.4 IT-Anwendungen inventarisieren und überwachen M.5 Anweisung zentraler Betrieb von IT-Fachverfahren einhalten M.6 Festplattenverschlüsselung einsetzen M.7 Mobile Device Management (MDM) einsetzen (…)	---	gr
2 VB VT	AL	**Datenverlust** Papiergebundene Daten können verloren gehen.	# Personal # Dritte (Dienstleister im Haus, Besucher) # Elemente (Wasser, Feuer)	Durch diverse Ereignisse (z.B. Diebstahl, Verlust auf Transportweg, Feuer) können Daten, die sich in Papierform an einem BAP befinden oder zwischen zwei BAP von einem Beschäftigten transportiert werden, unerwünscht verloren gehen.	Aus Erfahrungsberichten und Veröffentlichungen zu anderen Institutionen ist eine nicht geringe Wahrscheinlichkeit gegeben.	2		4	8	M.8 Absperrbares Aktenaufbewahrungsbehältnis nutzen M.9 Raum absperren M.10 Papierunterlagen inventarisieren M.11 E-Akte weiter ausbauen M.12 Selbsttransport reduzieren und absichern (…)	---	ge
5 VT DI	AL	**Unbefugte Verarbeitung** Über den IT-Arbeitsplatzrechner können **elektronische** Daten oder am **Bildschirm** dargestellte Daten unbefugt verarbeitet werden.	# IT-Fehlfunktion # Personal # Dritte # Straftäter	Beim Bildschirmarbeiten werden regelmäßig alle verarbeitete Daten am Monitor ausgegeben und können daher potenziell von anderen Personen unbefugt verarbeitet werden. Zudem könnte auf die elektronischen Daten des Arbeitsplatzrechners auch auf andere Art und Weise unbefugt zugegriffen und somit Daten unbefugt etwa eingesehen oder verändert werden.	Einige BAP befinden sich in Räumen mit regen Parteiverkehr (z.B. Bürger- und Unternehmensvertreter). Zudem steigt die Wahrscheinlichkeit von IT-Angriffsversuchen.	4		4	16	M.13 Bildschirm nur für Befugte lesbar gestalten M.14 Zugang zum IT-Arbeitsplatzrechner absichern M.15 Schnittstellen der Endgeräte deaktivieren M.16 Verschwiegenheitspflicht des Personals gewährleisten M.17 Löschung vor Ersatz durchführen M.1 Anweisung zur Speicherung von Daten einhalten M.2 Anti-Schadsoftware-Schutz verwenden M.3 Beschäftigte sensibilisieren	---	ge

ID	AP	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
Ziel					Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
										M.6 Festplattenverschlüsselung einsetzen		
										(…)		
7 VT	AL	**Unbefugte Verarbeitung** Über den Arbeitsplatz können unbefugte Personen **akkustische** Daten verarbeiten.	# Personal # Dritte # Straftäter	Personen können unbefugt Gespräche mithören, in denen Daten besprochen werden. Zudem können Anrufer insbesondere unter Vortäuschung falscher Tatsachen oder durch manipulierende Fragetechnik unbefugt Zugriff auf Daten erhalten.	Einige BAP befinden sich in Räumen mit regen Parteiverkehr (z.B. Bürger- und Unternehmensvertreter) und in akkustisch nicht besonders abgesicherten Bereichen (z.B. offenes Fenster, mobiles Arbeiten während einer Dienstreise, Home Office). Es gab bereits Social Engineering Angriffe durch Anrufer.	3		4	12	M.18 Telefonate mittels Headset führen		
										M.19 Raum-Akkustik technisch und organisatorisch sicher gestalten		
										M.16 Verschwiegenheitspflicht des Personals gewährleisten	---	ge
										M.3 Beschäftigte sensibilisieren		
										(…)		
8 VT DI	AL	**Unbefugte Verarbeitung** Über den Arbeitsplatz können unbefugte Personen **papiergebundene** Daten verarbeiten.	# Personal # Dritte # Straftäter	Auch an den BAP werden papiergebundene Daten verarbeitet, die in unbefugte Hände gelangen und sogar unbefugt verändert werden könnnen. Zudem werden Unterlagen mit Daten ausgedruckt und verbleiben längere Zeit am Drucker, wodurch Unbefugte einen Zugriff darauf erhalten könnten.	Aus Erfahrungsberichten und Veröffentlichungen zu anderen Institutionen ist eine nicht geringe Wahrscheinlichkeit gegeben.	3		4	12	s.o. Maßnahmen RM-ID 2.		
										M.20 Ausdruck via PIN		
										M.21 Ausdruckfunktion für Arbeitsplatz-Typen H* und M* gesperrt	---	ge
										M.22 Druckerräume abgesperrt von öffentlich zugänglichen Bereichen		
										M.3 Beschäftigte sensibilisieren		
										(…)		
(…)		**usw.** (…)	usw.	usw.	usw.	4	usw.	4	16	usw.		
										(…)		ro

Zielerfüllungsmanagement

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
DM - Datenminimierung IV - Intervenierbarkeit KE - Konzepteinhaltung NV - Nichtverkettung RI - Richtigkeit TP - Transparenz	**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**	ge

ID / Ziel	AP	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung: Erläuterung	Gefährdungsbewertung: Index	Maßnahme-Bezeichnung	Gefährdungsbewertung: Erläuterung	Gefährdungsbewertung: Index
1 DM	AL	**Datenüberhang** Es können Daten verarbeitet werden, deren Verarbeitung noch nie erforderlich war. **Datenlöschung** Es können Daten verarbeitet werden, die insbesondere seit dem schon erfolgten Wegfall bzw. der Erreichung des Verarbeitungszwecks bereits gelöscht sein müssten.	# IT-User # Personal # IT-Fehlfunktion	Beschäftigte und/oder befugte Externe (externe Experten wie Auditoren, Dienstleister usw.) verarbeiten auf dem BAP nicht (mehr) erforderliche Daten. Zudem kann vorkommen, dass ein IT-System automatisiert Daten auf dem IT-Arbeitsplatzrechner mit einer vergleichbaren Problematik speichert.	Der Anreiz ist wahrnehmbar, elektronische Daten mal schnell auf den IT-Arbeitsplatzrechner selbst zu speichern und papiergebundene Daten, deren Bearbeitung nicht (mehr) erforderlich ist, etwa in der Form von "Schattenakten" am Arbeitsplatz zu verarbeiten. Zudem gibt es IT-Systeme, die - wenn auch nur temporär - automatisiert Daten auf dem IT-Arbeitsplatzrechner ablegen.	ro	M.23 Auftragsverarbeiter unterweisen M.24 Festplatte nach Auffälligkeiten scannen. M.25 Systemlieferanten nach Speicherfunktion fragen M.1 Anweisung zur Speicherung von Daten einhalten M.3 Beschäftigte sensibilisieren M.11 E-Akte weiter ausbauen M.26 Stichprobenprüfung systematisch durchführen M.30 Datenexport von IT-Anwendungen auf das Notwendige beschränken (…)	---	ge
2 IV	AL	**Automatisierte Entscheidung** Betroffene Personen können ihr Recht auf Abwehr automatisierter Entscheidungen im Einzelfall nicht wahrnehmen (Art. 22 DSGVO).	# Personal	Ein ordnungsgemäß geltend gemachter Anspruch auf Abwehr automatisierter Entscheidungen wird nicht erfüllt.	An BAP gibt es keine automatisierten Entscheidungen, wie diese vorausgesetzt werden.	---	---	---	---
		Auskunft Betroffene Personen können ihr Recht auf Auskunft nicht wahrnehmen (Art.15 DSGVO). **Berichtigung** Betroffene Personen können ihr Recht auf Berichtigung nicht wahrnehmen (Art.16 DSGVO).					s.o. Maßnahmen zur Einzelgefährdungs-ID 1. M.28 Elektronische Protokollierung des IT-Arbeitsplatzrechner konfigurieren M.29 Telemetriedaten des IT-Arbeitsplatzrechners verhindern (…)		

ID / Ziel	AP	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
					Erläuterung	Index		Erläuterung	Index
3 IV TP NV	AL		# IT-User # Personal # IT-Fehlfunktion	Es werden Daten am BAP verarbeitet, die unerfasst und damit ohne Kenntnis des Verantwortlichen verarbeitet werden. Damit werden diese Daten insbesondere nicht durch die Geschäftsprozesse des Datenschutz-Managements erfasst, das Garant beispielsweise für die wirksame Durchsetzung der Betroffenenrechte ist.	Der Anreiz ist wahrnehmbar, elektronische Daten mal schnell auf den IT-Arbeitsplatzrechner selbst zu speichern und papiergebundene Daten, deren Bearbeitung nicht (mehr) erforderlich ist, etwa in der Form von "Schattenakten" am Arbeitsplatz zu verarbeiten. Zudem gibt es IT-Systeme, die - wenn auch nur temporär - automatisiert Daten auf dem IT-Arbeitsplatzrechner ablegen.	ro		---	ge
		Löschung Betroffene Personen können ihr Recht auf Löschung nicht wahrnehmen (Art. 17 Abs. 1 DSGVO).							
		Einschränkung Betroffene Personen können ihr Recht auf Einschränkung der Verarbeitung nicht wahrnehmen (Art. 18 DSGVO).							
		Datenübertragbarkeit Betroffene Personen können ihr Recht auf Datenübertragbarkeit nicht wahrnehmen (Art. 20 DSGVO).							
		Widerspruch Betroffene Personen können ihr Recht auf Widerspruch nicht wahrnehmen (Art. 21 Abs. 1 Satz 1 DSGVO).							
4 TP	AL	**Information** Die Informationspflichten nach Art. 13, 14 DSGVO werden nicht (vollständig) erfüllt.							
5 NV	AL	**Zweckentfremdung** Die Daten können rechtswidrig für einen anderen Zweck verarbeitet werden.							
6 KE	AL	**Aktualität Konzepte** Die relevanten Vorgaben für die Prozesse und sie unterstützende Systeme, die an der Verarbeitung der Daten beteiligt sind, können veraltern und damit nicht mehr gültig sein.	# Personal	Der Nachweis einer ordnungsgemäßen Verarbeitung kann nicht erbracht werden.	Die Synchronisation der dokumentierten Konzeption und der tatsächlichen Umsetzung ist nicht immer gegeben.	ro	M27 Veränderungsmanagement durchführen (…)		ro
(…)	(…)	**usw.** (…)	(...)	(...)	(...)	ro	(...)	(...)	ro

Schutzmaßnahmen (TOMs)

ID	AP	Bezeichnung	Kurzbeschreibung	Verweise	Anmerkungen
M.1	AL	Anweisung zur Speicherung von Daten einhalten	Durch die Anweisung wird u.a. festgelegt, dass Daten nicht auf dem IT-Arbeitsplatzrechner originär gespeichert werden dürfen.	//Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.2	AL	Anti-Schadsoftware-Schutz verwenden	Alle IT-Bildschirmplätze sind mit einem Anti-Schadsoftware-Schutzsystem für Endgeräte ausgestattet, das u.a. eine zentrale Überwachungsfunktion hat.	// Spezifikation Anti-Malware-Schutzsystem (Dok-ID 2644)	
M.3	AL	Beschäftigte sensibilisieren	Sensibilisierungskonzept für Datenschutz und IT-Sicherheit beinhaltet auch, wie Beschäftigte am IT-gestützten Arbeitsplatz mit Daten umgehen müssen.	// Konzept Schulung und Sensibilisierung bzgl. Datenschutz (Dok-ID 2644) und IT-Sicherheit (Dok-ID 2645).	
M.4	AL	IT-Anwendungen inventarisieren und überwachen	Durch einen geeigneten und laufend aktuell gehaltenen Überblick über alle IT-Anwendungen, die auf den Bildschirmarbeitsplätzen verfügbar sind, können insbesondere deren Konfigurationen bzgl. Datenspeicherort gesteuert werden.	// Spezifikation Enterprise Architecture Management (EAM), mit dem alle IT-Anwendungen verwaltet werden (Dok-ID 68346).	
M.5	AL	Anweisung zentraler Betrieb von IT-Fachverfahren einhalten	IT-Fachanwendungen dürfen grundsätzlich nur auf zentral betreuten Servern zusammen mit ihren Fachdaten betrieben werden.	//Anweisung Betrieb von IT-Fachverfahren (Dok-ID 36)	
M.6	H* M* *P	Festplattenverschlüsselung einsetzen	Lokalen Speicher (Festplatte, SD usw.) des Arbeitsplatzrechners sowie weitere Datenträger verschlüsseln.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123).	
M.7	H* M*	Mobile Device Management (MDM) einsetzen	Für mobile Endgeräte wird MDM genutzt.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123).	
M.8	B* H*	Absperrbares Aktenaufbewahrungsbehältnis nutzen	Papierunterlagen mit Daten müssen beim längeren Verlassen des IT-Arbeitsplatzes in absperrbare Aktenaufbewahrungsbehältnisse (z.B. Aktenschrank, Rollcontainer) eingeschlossen werden.	//Anweisung Umgang mit Papierunterlagen am Arbeitsplatz (Dok-ID 2666).	
M.9	B*	Raum absperren	Beim Verlassen des IT-Arbeitsplatzes und als letzter Beschäftigter im Raum wird der Raum abgesperrt.	//Anweisung Umgang mit Papierunterlagen am Arbeitsplatz (Dok-ID 2666).	
M.10	AL	Papierunterlagen inventarisieren	Papierunterlagen werden möglichst früh im Aktensystem erfasst und inventarisiert.	//Spezifikation Registratursystem (Dok-ID 2668) und //Anweisung Posteingang (Dok-ID 2669).	
M.11	AL	E-Akte weiter ausbauen	Der rasche Ausbau der E-Akte wird zur deutlichen Reduktion von Papierunterlagen führen.	Projekt "Ausbau der E-Akte" (Dok-ID 20190302).	
M.12	H* M*	Selbsttransport reduzieren und absichern	Papiergebundene Daten dürfen ab einen klar festgelegten Schutzbedarf die Dienststelle nicht verlassen. Unverzichtbare sonstige Transporte sind geeignet abzusichern (z.B. Transport von Kopien, Transportbehältnis absperrbar und nach Verlust einfach rücksendbar für Finder gestalten).	//Anweisung Transport von Unterlagen außerhalb der Dienststelle.	
M.13	AL	Bildschirm nur für Befugte lesbar gestalten	Die Anzeige Daten am Bildschirm wird insbesondere durch Sperren des Arbeitsplatzrechners beim Verlassen des Arbeitsplatzes, geeignete Ausrichtung des Bildschirms und ggf. Sichtschutzfolien abgesichert.	//Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.14	AL	Zugang zum Arbeitsplatzrechner absichern	Alle städtischen Arbeitsplatzrechner sind insbesondere mit einer 2-Faktor-Authentifizierung (persönliche PIN und Smartcard) schon für die "Basisanmeldung" ausgestattet. Zudem besteht Anweisung, dass der Arbeitsplatzrechner vor Verlassen des IT-Arbeitsplatzes zu sperren ist, so dass nach einer Rückkehr wiederum die Basisanmeldung für einen Zugang erforderlich ist.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123) und //Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.15	AL	Schnittstellen der Endgeräte deaktivieren	Nicht benötigte Schnittstellen der Endgeräte (z.B. Arbeitsplatzrechner) werden deaktiviert (z.B. USB).	//Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.16	AL	Verschwiegenheitspflicht des Personals gewährleisten	Die Beschäftigten der Stadt sind ab Beginn ihres Dienst- bzw. Arbeitsverhältnisses von Gesetzes wegen verpflichtet, das Datengeheimnis zu beachten. Bei Aufnahme einer Tätigkeit für die Stadt Fiktivia werden Beschäftigte über ihre Pflichten hinsichtlich des Schutzes personenbezogener Daten erstmalig informiert.	//Anweisung Geschäftsprozess "Onboarding durchführen" (Dok-ID 20190503).	

ID	AP	Bezeichnung	Kurzbeschreibung	Verweise	Anmerkungen
M.17	AL	Löschung vor Ersatz durchführen	Werden Arbeitsplatzrechner und relevante Teile daraus (z.B. lokale Festplatte, SD) oder sonstige relevante Technik (z.B. Telefon, Aktenschrank) insbesondere aufgrund Mangelbeseitigung oder Ende der Lebensdauer ersetzt oder aus einem anderen Grund Dritten zur Verfügung gestellt, werden zuvor eventuell noch bei den Austauschobjekten vorhandene Daten gelöscht bzw. entfernt.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123) und //Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.18	AL	Telefonate mittels Headset führen	Dort, wo entsprechende Risiken gesehen werden, erhalten die Beschäftigten Headsets zum Telefonieren.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123) und //Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.19	B*	Raum-Akkustik technisch und organisatorisch sicher gestalten	Das bestehende Raumkonzept und die sich daraus ergebenden Maßnahmen gewährleisten u.a., dass über geeignete Abstände, technische Akkustikmaßnahmen usw. das gesprochene Wort geschützt wird.	//Konzept Raumkonzept (Dok-ID 20170320).	
M.20	B*	Ausdruck via PIN	Wählbare Druckaufträge werden erst durch Freigabe mittels einer geheimen PIN am Drucker ausgedruckt.	//Anweisung IT-Dienstanweisung (Dok-ID 20170320).	
M.21	H* M*	Ausdruckfunktion für Arbeitsplatz-Typen H* und M* gesperrt	Sobald ein Arbeitsplatzrechner sich nicht mehr im Dienstgebäude befindet, wird die Ausdruck-Funktion automatisiert deaktiviert.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123).	
M.22	B*	Druckerräume abgesperrt von öffentlich zugänglichen Bereichen	Die Druckerräume sind gegen Zugang von nicht befugten Personen technisch und organisatorisch abgesichert.	//Konzept Raumkonzept (Dok-ID 20170320).	
M.23	AL	Auftragsverarbeiter unterweisen	In Auftragsverarbeitungsvereinbarungen (AVV) auf die Einhaltung datenschutzrechtlicher Anforderungen standardmäßig hinweisen sowie Auftragsverarbeiter vor Aufnahme ihrer Tätigkeit entsprechend unterweisen.	//Anweisung Geschäftsprozess "IT-Dienstleister einsetzen" (Dok-ID 20170507) und //Muster AVV (Dok-ID 20180609).	
M.24	AL	Festplatte nach Auffälligkeiten scannen	Jährlich werden die lokalen Speicher (Festplatte, SD usw.) der IT-Arbeitsplätze in den dienstlichen Speicherbereichen nach Auffälligkeiten gescannt.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123).	
M.25	AL	Systemlieferanten nach Speicherfunktion fragen	Vor Installation neuer IT-Systeme auf den Arbeitsplatzrechnern werden die Lieferanten nach dem Speichermanagement Daten befragt und insbesondere, ob etwa eine IT-Anwendung automatisiert und temporär Daten auf dem lokalen Speicher des Arbeitsplatzrechners ablegen.	//Anweisung Geschäftsprozess "IT-Beschaffung durchführen" (Dok-ID 20170507) und //Muster IT-Vertrag (Dok-ID 20180609).	
M.26	AL	Stichprobenprüfung systematisch durchführen	Führungskräfte sind angewiesen, bei ihrem Personal bedarfsgerecht Stichproben auch auf Einhaltung der datenschutzrechtlichen Vorgaben zum IT-Arbeitsplatz durchzuführen. Zudem gehören die Vorgaben zum IT-Arbeitsplatz ausdrücklich zum Prüfungsumfang der städtischen internen Revision.	//Anweisung Geschäftsprozess "Personal führen" (Dok-ID 20180507) und //Anweisung Geschäftsprozess "Revisionsprüfungen durchführen" (Dok-ID 20180909).	
M.27	AL	Veränderungsmanagement durchführen	Relevante Veränderungen werden systematisch von Beginn an erfasst und in die einschlägigen Konzepte (Dokumantation) aufgenommen.	//Anweisung Geschäftsprozess "Änderungen durchführen" (Dok-ID 20180508).	
M.28	AL	Elektronische Protokollierung des IT-Arbeitsplatzrechner konfigurieren	Die elektronische (automatisierte) Protokollierung des IT-Arbeitsplatzrechners ist insbesondere Umfang, Zugriff und Aufbewahrungszeitraum klar festgelegt.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123).	
M.29	AL	Telemetriedaten des IT-Arbeitsplatzrechners verhindern	Die Anforderungen des DSK-Beschlusses "Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise" vom 26.11.2020 sind umgesetzt.	//Spezifikation Arbeitsplatzrechner (Dok-ID 20130123).	
M.30	AL	Datenexport von IT-Anwendungen auf das Notwendige beschränken	Ein möglicher Datenexport etwa aus IT-Fachverfahren (z.B. HCM) sollte grundsätzlich deaktiviert sein.	Spezifikation aller einschlägigen Betriebsmittel.	
M.31	(…)	(…)	(…)	(…)	