Es muss festgelegt und dokumentiert sein:							
- wer und wie Personalwechsel melden muss bzw. die Befugnis hat; z. B. die Personalverwaltung per Formular an die IT							
- wer (Personalstelle und/oder Fachabteilung) welche Angaben liefern muss							
- wer (IT, externer Dienstleister, ISB) welche Tätigkeiten durchzuführen hat							

		Neuanlage	interner Wechsel	Ausscheiden	**Checkliste Mitarbeiter*innen-Wechsel** **als Unterstützung zur Erstellung eines auf Ihre Kommune abgestimmten Ablaufs / Laufzettels oder Formular für IT, ISB, DSB, Personalverwaltung**	Erledigt	Dokumentiert
1.1	1. Angaben zur Person	x	x	x	Angabe von Name und Vorname, oft Personalnummer. Evtl. Amtsbezeichung. Konto im Verzeichnisdienst / Active Directory anlegen / umziehen / löschen. Eine zeitliche Befristung muss angegeben werden und wird am Konto hinterlegt. Bei Fremdpersonal grundsätzlich zeitliche Befristung (Kontoablauf).		
1.2		x	x	x	Anmeldename: Namenskonventionen beachten. Umlaute, maximale Länge, ggf. Mindestlänge, Umgang mit Doppelnamen, Umgang mit Titeln (z. B. Doktor)		
1.3		x	x		Straße und PLZ (vor allem bei Außenstellen). Etage, Zimmer-Nr.		
1.4		x	x	x	Name des Rechners / Notebooks? Dienstliche Mobiltelefonnummer?		
1.5		x	x	x	Telefon-Nr einrichten oder stilllegen, ggf. Anrufbeantworter, Fax, VoIP-/CTI-Konfiguration.		
2.1	2. Angaben zur Abteilung		x	x	Alte Dienststelle / Abteilung / Referat /OrganisationUnit (OU)		
2.2		x	x		Neue Dienststelle / Abteilung / Referat / OU		
2.3		x	x	x	Zeitpunkt der Änderung beachten (ggf. Konto an einem Stichtag aktivieren/deaktivieren). Konten sollten auch für Beurlaubungen, Elternzeit, Pflegezeiten deaktiviert werden). Sonderfall: User hilft noch im alten Tätigkeitsbereich aus (Überschneidung Laufwerksbuchstaben-Zuweisung durch GPO oder Loginscript prüfen).		
3.1	3. (AD-) Gruppen		x	x	Alte Gruppen entfernen, Zeitpunkt, evtl. Überlappung mit neuer Gruppenzugehörigkeit		
3.2		x	x		Neue Gruppenmitgliedschaften eintragen		
4.1	4. E-Mail	x	x	x	E-Mail-Postfach einrichten / ggf. umziehen / löschen (hier: Autoresponder falls gewünscht)		
4.2		x	x		Mail-Archivordner vorhanden (Bei MS Outlook *.PST)? Speicherort, Datenübernahme, evtl. aufteilen/komprimieren		
4.3			x	x	Alte Verteilergruppen prüfen (DL = distribution list), ist der wechselnde/ausscheidene User die letzte Person in der Verteilergruppe?		
4.4		x	x		Neue Verteilergruppe		
4.5		x	x	x	Stellvertretung einrichten / aufheben		
4.6		x	x		Postfachberechtigungen (beim Ausscheiden erlöschen die Rechte i. d. R. durch das Löschen des Postfaches)		
4.7		x	x		Rechte auf Funktionspostfächer (SharedMailbox / öffentl. Ordner), E-Mail-, Kalender- & Kontakte-Ordner. Verknüpfungen auf Outlookleiste des Users / Einbindungen löschen		
5.1	5. Daten	x	x	x	Homelaufwerk / Basisverzeichnis AD: Einrichten / ggf. umziehen / löschen		
5.2		x	x	x	ggf. weitere Netzlaufwerke, Rechte. Ggf. vorhandene Cloudspeicher beachten.		
5.3		x	x	x	ggf. Loginscript anpassen		
5.4		x	x	x	Arbeitszeitaufschreibungen (wenn keine zentrale Arbeitserfassung)		
5.5			x	x	Lokale Daten auf dem alten Rechner / Notebook? Neuinstallation des Altrechners?		
5.6		x	x	x	personalisierte Zugänge zu Webseiten und Gremien übergeben / umschreiben / löschen. Ggf. Übergabe von Kennwörter / Passwortspeicher oder Umregistrierung auf Funktionsadressen oder Nachfolger. Änderung von Passwörtern, damit der ausscheidene User keinen Zugriff mehr auf Ressourcen des bisherigen Tätigkeitsbereichs mehr hat. Wissenstransfer, vor allem für geschäftskritische Prozesse.		
5.7		x	x	x	Beim Ausscheiden von IT-Administratoren: - personalisierte Administrationszugänge löschen - Änderung Passwörter/Zugangslogiken, die der Admin darüber hinaus noch kennt - Information der Benutzer über das Ausscheiden des bisherigen Administrators - Bei Benennung gegenüber Dritten, z. B. in Verträgen oder als Internetdomain-Admin-C: Festlegung neuer Ansprechpartner sowie Information der betroffenen Dritten.		

5.8		x	x	x	Zugänge für sicherheitskritische Bereiche (z. B. BayBIS, eKol, inPol, Condition) oder Geheimschutz (VS-NfD) löschen bzw. neu initialisieren. Bei Neuzugang notwendige Einweisungen (Tätigkeiten, IT-Architektur, zu betreuende Systeme und Anwendungen, geltende Regelungen und Sicherheitsbestimmungen).		
5.9		x	x	x	Pflege von Datenverzeichnissen, auch Mitarbeiterinfos und Telefonverzeichnis im Intranet, Zuständigkeitshinweise im Internet. Ggf. Visitenkarten - alte Karten beim Ausscheiden vernichten.		
6.1	6. Benutzerprofil	x	x	x	Servergespeichert: anlegen/löschen, ggf. teilweise umziehen (Favoriten, Desktop, Eigene Dateien, falls keine Ordnerumleitung), AD-Profilpfad eintragen/ändern		
6.2			x	x	Lokal: Daten daraus noch erforderlich?		
6.3		x	x	x	Terminalserver-Profil? (AD-Konsole, Reiter Remotedesktopdienste-Profil) VDI-Umgebung? Daten?		
6.4		x	x		Anleitung für das Einrichten von Netzwerkdruckern am Printserver, vertraulicher Druck? Ggf. Kostenstelle.		
7.1	7. Hardware	x	x	x	Mobiliar vorhanden? Ggf. beschaffen. Schlüssel für Möbel ausgeben / einziehen. Aufstellung gemäß Arbeits- und Datenschutz, auf unbefugte Einsichtsmöglichkeiten in Monitore achten, notfalls Blickschutzfolie. Ggf. Raum-Management (datenschutzgerechtes Tür-Namensschild, Umzug).		
7.2		x	x	x	Telefon vorhanden / beschaffen / konfigurieren. Kurzwahlfunktion für IT-Notfall.		
7.3		x	x	x	PC: geeigneter Rechner/Peripherie vorhanden / beschaffen / neu installieren / "abziehen". Ggf. vorhandene persönliche Hardware berücksichtigen (Blinde / User mit Handicap).		
7.4		x	x	x	NB: geeigneter Notebook (Dockingstation, Adapter) vorhanden / beschaffen / neuinstallieren / abziehen. PIN für Bitlocker. Außendienst: Tarif und PIN für SIM-Karte. Entsperrcodes. Telearbeit / VPN?		
7.5		x	x	x	Mobilgeräte: Mobiltelefone, Tablets beschaffen / neu konfigurieren / abziehen. Tarif und PIN für SIM-Karte. Entsperrcodes (PUKs). Zugelassene Apps (MDM).		
7.6		x	x	x	Falls 2-Faktor-Authentifizierung: Geräte wie RSA-Token beschaffen / konfigurieren / einziehen. Ggf. Anleitung, PIN-Code.		
7.7		x	x	x	Chipkarten für Zugänge (Türen), PKI (Signatur/Verschlüsselung), vertraulicher Druck. Beim Wechsel / Ausscheiden einziehen, bei Verlust Zertifikate sperren.		
7.8		x	x	x	Schlüssel, Transponder (falls kein Zugang mit Chipkarte): Ausgeben, beim Wechsel / Ausscheiden umprogrammieren / einziehen, bei Verlust sperren. Zimmer / Schließkreis.		
7.9		x	x	x	Dienstausweis: ausstellen, bei Wechsel / Ausscheiden einziehen, bei Verlust sperren.		
7.10		x	x	x	mobile Datenträger wie USB-Sticks, Festplatten, SSDs: Ausgeben / löschen / einziehen. Autarke Dateien von vorhandenen Datenträgern sichern.		
8.1	8. Software	x	x	x	Betriebssystem/Programme wie Office: Lizenzen beschaffen / ggf. übertragen, installieren, deinstallieren Ggf. vorhandene persönliche Software berücksichtigen (Blinde / User mit Handicap)		
8.2		x	x	x	Fachverfahren: Benutzer-Konto? Administrator-Konto? Lizenzen? Dongle? Weitere Konten, z. B. WiKi oder E-Akte (Rolle des Users?)		
9.1	9. Awareness	x			Erstunterweisung IT-Sicherheit, Unterweisung für den neuen Aufgabenbereich, Verpflichtung auf Datenschutz und ggf. Fachgesetze. Ggf. Anmeldung zu Schulungen.		
9.2			x		Unterweisung für den neuen Aufgabenbereich, ggf. Verpflichtung auf Fachgesetze. Ggf. Anmeldung zu Schulungen.		
9.3		x	x	x	Hinweise auf Vertraulichkeitsvereinbarungen		
Hinweise:							
Ggf. Wartezeiten für Importvorgänge beachten (z. B. Aktualisierung von Konten von einem System in ein anderes über Nacht).							
Ggf. Checkliste für Telearbeit erweitern.							
Besonderes Augenmerk bei Fremdpersonal, auch hier Vertraulichkeitsvereinbarungen.							
Bei Abmahnung, Beweissicherungsverfahren, Kündigung: Vor Eröffnung den Entzug von Zutritten, Zugängen und Zugriffen prüfen.							
Wenn Personal wechselt oder ausscheidet, haben sich Formblätter bewährt, was von diesem Personenkreis erwartet wird, wie							
z. B. das Leeren des Homelaufwerks oder Abgeben von Notebooks. Diese Informationen sollten rechtzeitig versandt werden.							
Für jegliche Hardware:					Default-Passwörter ändern, ggf. Update Firmware / EFI bzw. BIOS und Inventarisierung.		
					Bei Servern: Festlegen und Dokumentation der Verantwortlichen und Aufnahme ins Monitoring.		
Für jegliche Software:					Lizenz-Inventarisierung.		
					Default-Passwörter ändern bei Erst-Installationen von Datenbanken, Instanzen, Apps und Fachverfahren.		
Siehe auch BSI-IT-Grundschutz ORP.2 Personal, ORP.4 Identitäts- und Berechtigungsmanagement, für Administratoren OPS.1.1.2.A3, A4							