RUHR UNIVERSITÄT BOCHUM

Onboarding und Informationssicherheit

Eine Checkliste für Führungskräfte

Die Einbindung der Informationssicherheit in den Onboarding-Prozess trägt dazu bei, dass neue Mitarbeitende gut vorbereitet sind, um die Sicherheit und Integrität der Informationen zu gewährleisten. Informationssicherheit ist aber mehr als der Schutz sensibler Daten oder IT-Security. Informationssicherheit schafft ein Verantwortungsbewusstsein, gewährleistet die Einhaltung gesetzlicher Vorschriften, ist die Grundlage für eine organisationale Sicherheitskultur und schafft so Vertrauen in die Organisation und verringert die Gefahr von Sicherheitsvorfällen.

Hier finden Sie wichtige Aspekte und Empfehlungen für die Bereiche Infrastruktur, Zutrittskontrollen, Identitäts- und Zugriffsmanagement, IT-Systeme und Anwendungen, technische Sicherheitsmaßnahmen sowie Sensibilisierungen, die Sie im Rahmen des Onboardings berücksichtigen sollten.

Was ist zu tun			
✓	**Vor dem ersten Arbeitstag?**	**Bereich**	**Interne Hilfen**
☐	Auswahl des Arbeitsplatzes: Vermeidung von Büroräumen mit Publikumsverkehr in sicherheitsrelevanten Bereichen.	**Infrastruktur**	
☐	Beantragung von Zutrittskontrollmitteln (Schlüssel/Transponder).	**Zutrittskontrolle**	**Schließtechnik**
☐	Festlegung und Dokumentation der Zutrittsrechte → Vergabe der Rechte nach dem Least Privileges Prinzip und Funktionsgebunden. Dabei sicherstellen, dass keine Rollenkonflikte vorliegen.	**Zutrittskontrolle**	**FAQ Schließtechnik**
☐	Bereitstellung und Einrichtung von EDV-Ausstattung (PC, Laptop, mobile Endgeräte, Drucker, etc.).	**Technische Sicherheitsmaßnahmen**	**Checkliste zur Grundsicherung**
☐	Beantragung einer neuen LoginID.	**Identitäts- & Zugriffsmanagement**	**IT.SERVICES – LoginID und MFA**

	Festlegung und Dokumentation der Gruppenzugehörigkeit und Rechtevergaben. → Rechte nach dem Least Privileges Prinzip und funktionsgebunden vergeben. Sicherstellen, dass keine Rollenkonflikte vorliegen.	**Identitäts- & Zugriffsmanagement**	
	Freischaltung der LoginID und Prüfung der Zugangs- und Zugriffsrechte.	**Identitäts- & Zugriffsmanagement**	**IT.SERVICES – LoginID und MFA**
	Individuelle Einrichtung von IT-Systemen und Anwendungen.	**IT-System und Anwendung**	
	Einrichtung von Netzwerkzugriffen und Einbindung von Laufwerken.	**IT-System und Anwendung**	
	Freigabe von Ordnern und Bereitstellung benötigter Softwarelizenzen.	**IT-System und Anwendung**	**Software-Angebot von IT.SERVICES**
	Aushändigung erforderlicher Informationen zu Ansprechpartnern, Gesetzen, Regelungen, Datenschutz, Datensicherungskonzepten, etc.	**Sensibilisierung**	**Seiten des DSB und Seiten der ISB**
✓	**Gut zu wissen: Regelungen und sichere Praxis**	**Bereich**	**Interne Hilfen**
	Einhaltung der Brandschutzvorschriften und Bauaufsicht-Auflagen.	**Infrastruktur**	**AGUM-Portal Formularcenter**
	Umsetzung und Einhaltung der Arbeitsstätten-verordnung.	**Infrastruktur**	**AGUM-Portal Formularcenter**
	Sicherstellen, dass Räume verschlossen werden, wenn vertrauliche Informationen zurückgelassen werden.	**Infrastruktur & IT-System und Anwendung**	
	Schutz des Arbeitsplatzes bei kurzzeitigem Verlassen durch Schließen von Fenstern und abschließen der Tür.	**IT-Systeme und Anwen-dung & Technische Sicherheitsmaßnahmen**	
	Sicherstellung, dass vertrauliche Gespräche nicht abgehört werden können.	**Infrastruktur**	
	Bildschirme vor unbefugtem Einsehen schützen.	**Infrastruktur**	
	Fenster und Türen bei Nichtbesetzung des Raumes schließen.	**Infrastruktur**	
	Dokumentierte Übergabe und Schulung im sicheren Umgang mit Zutrittskontrollmitteln.	**Zutrittskontrolle**	**FAQ Schließtechnik**
	Zutrittskontrollmittel nicht weitergeben oder ungeschützt am Arbeitsplatz hinterlassen.	**Zutrittskontrolle**	
	Kontaktperson bei Schließtechnikproblemen bereitstellen.	**Zutrittskontrolle**	**Schließtechnik**
	Festlegung eines neuen Passworts nach der Passwortrichtlinie.	**Identitäts- & Zugriffs-management und IT-System und Anwendung**	**Passworthinweise ISB**

	Passwörter nicht weitergeben oder ungeschützt am Arbeitsplatz hinterlassen.	**Identitäts- & Zugriffsmanagement**	**Passworthinweise ISB**
	Kontaktperson bei Authentifizierungsproblemen bereitstellen.	**Identitäts- & Zugriffsmanagement**	**IT.SERVICES-Helpdesk**
	Prüfung der erhaltenen Zugangs- und Zugriffsrechte.	**IT-System und Anwendung**	
	Installation von Software unter Abwägung der potenziellen Risiken und Sicherstellung der Nutzungsberechtigungen.	**IT-System und Anwendung**	**Software-Angebot von IT.SERVICES**
	Meldung von IT-sicherheitsrelevanten Vorfällen an die zuständige Beauftragte für Informationssicherheit.	**IT-System und Anwendung & Technische Sicherheitsmaßnahmen**	**Sicherheitsvorfälle melden**
	Sicherung dienstlich relevanter Datenbestände abhängig vom Schutzbedarf.	**Sensibilisierung**	
	Ablage dienstlich relevanter Datenbestände im Verantwortungs- und Zugriffsbereich der Ruhr-Universität Bochum. → KEINE private Hard-/Software, KEINE privaten Speichermedien	**Sensibilisierung**	
	Berücksichtigung des Schutzbedarfs und rechtlicher Anforderungen bei der Nutzung von dienstlichen Cloud-Diensten.	**Sensibilisierung**	
✓	**Gut zu wissen: Schulungsangebote**	**Bereich**	**Interne Hilfen**
	Schulung zu allgemeinen Regeln am Arbeitsplatz.	**Infrastruktur**	**AGUM-Portal Formularcenter**
	Schulung im sicheren Umgang mit Authentifizierungsmerkmalen.	**Identitäts- & Zugriffsmanagement**	**IT.SERVICES – LoginID und MFA**
	Teilnahme an Schulungen im sicheren Umgang mit IT.	**Technische Sicherheitsmaßnahmen**	**Fortbildungsportal**
	Schulung im sicheren Umgang mit IT → Teilnahme am SecAware-Moodle-Kurs	**Sensibilisierung**	**SecAware-Kurs in Moodle**