Kommunen & Behörden

GATACA® Datenschutz GmbH

Frage des CSBW	Antwort	Check
Ist für die Kommune eine oder ein interne/r oder externe/r ISB ernannt und koordiniert erste Sicherheitsmaßnahmen?	Bestellen Sie einen Fachkundigen ISB. *Ein ISB strukturiert nicht nur Ihre Informationssicherheit und treibt dies voran, sondern ist auch Ansprechpartner und Berater. Gern unterstützt GATACA durch das stellen des DSB Ihre Kommune/Behörde.*	☐
Ist für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen festgelegt worden, wer für diese und deren Sicherheit zuständig ist?	Zuständigkeit ist ein Thema das für Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen geregelt werden muss.	☐
Sind verbindliche Regelungen für die Informationssicherheit festgelegt und an alle Mitarbeitenden kommuniziert worden? Ist sichergestellt, dass auch alle Neueinstellungen über diese Regelungen informiert werden?	Regeln müssen aufgestellt und kommuniziert werden. Wenn hierbei noch der Hintergrund, vordem diese Regeln entstanden sind, erklärt wird erhöht dies die Akzeptanz erheblich. Hier stellt GATACA Ihnen unten eine Checkliste zur Verfügung welche Regeln Sie auf jeden Fall aufstellen sollen. (Nur die wichtigsten.)	☐
Gibt es Checklisten, was beim Austritt von Beschäftigten zu beachten ist (Anfertigung Dokumentation, Einweisung der oder des Nachfolgenden, Berechtigungen, Schlüssel, Information aller betroffenen Stellen, Anpassungen von Verantwortlichkeiten, etc.)?	Durch Checklisten bei einem Eintritt/Austritt und auch Positionswechsel vermeiden Sie Themen zu vergessen. Nutzen Sie hier unsere Checkliste, welche Sie auf der letzten Seite finden.	☐
Werden alle Mitarbeitenden (und Neueinstellungen) regelmäßig über die Gefahren beim Umgang mit IT-Geräten informiert?	In 95 % aller Fälle ist der Mitarbeiter die Ursache eines Sicherheitsvorfalles. Diese Zahl können Sie durch gute Schulungen senken. GATACA bietet eine Grundschulung für Datenschutz und Informationssicherheit für Kommunen und Behörden kostenlos an.	☐
Sind alle Mitarbeitenden der Kommune für den sicheren Umgang mit Passwörtern sensibilisiert (z.B. sichere Aufbewahrung am besten in einem sicheren Passwort-Manager)?	Das Thema Passwort ist leidig. Hier sollte man entweder eine Regel zu ausreichend komplexen Passwörtern einführen oder noch besser diese automatisch generieren. Passwörter sollten je nach Empflindlichkeit der Daten unterschiedlich komplex sein. Als Faustformel gilt ein Passwort als ausreichend komplex, wenn: 1. Zahlen, Sonderzeichen, Buchstaben, Groß- & Kleinschreibung enthalten sind. 2. Diese zufällig sind (keine Namen, Geburtstage, etc.) 3. Die Länge ausreichend ist (Wir empfehlen i.d.R. 12 Zeichen sofern nicht ein weiterer Faktor hinzukommt) Gut ist auch ein Passwortmanager. Hier berät Sie gerne einer unserer Kollegen und Kolleginnen unserer Schwester dem GATACA Systemhaus.	☐

Ist sichergestellt, dass regelmäßige Datensicherungen erstellt werden?	Ein Backup ist bei einem Informationssicherheitsvorfall (Cyberangriff; Schäden am Server, etc.) Ihre einzige Möglichkeit, Daten wiederherzustellen. Klar kann bei einem Angriff auch das Backup betroffen sein aber ohne Backup kennt die IT den unsäglichen Spruch: Kein Backup, kein Mitleid. Hier berät Sie gerne einer unserer Kollegen und Kolleginnen aus unserer Schwester dem GATACA Systemhaus.	☐
Gibt es einen vollständigen und aktuellen Netzplan?	Wie viele Endgeräte haben Sie. Wie sind Ihre Geräte miteinander verbunden. Eine Frage die Sie ins Grübeln bringt. Wie geht man hier vor. Händisch zählen? Warum ist das wichtig? Nur wenn Sie wissen was Sie haben, dann wissen Sie was Sie zu schützen haben. Hier berät Sie gerne einer unserer Kollegen und Kolleginnen aus unserer Schwester dem GATACA Systemhaus.	☐
Ist sichergestellt, dass Laptops nach aktuellem Stand der Technik verschlüsselt sind?	Die Absicherung Ihrer Endgeräte ist essentiell für Ihre Sicherheit. Sichern Sie Ihre Laptops mit einer Verschlüsselung. Hier berät Sie gerne einer unserer Kollegen und Kolleginnen aus unserer Schwester dem GATACA Systemhaus.	☐
Ist der Zugriff auf alle IT-Systeme und Fachanwendungen nur mit angemessener Identifikation und Authentisierung möglich (d.h. nur nach Eingabe einer individuellen Userid und Passwort ggfs. nach Multi-Faktor-Authentisierung)?	Kein Passwort ist vollständig sicher. Dieser Erkenntnis tragen Sie Rechnung indem Sie neben dem Passwort einen weiteren Faktor hinzunehmen. Beispielsweise ein nur für kurze Zeit gültiges weiteres Passwort welches dem Mitarbeiter auf dem Smartphone zugespielt wird. Hier berät Sie gerne einer unserer Kollegen und Kolleginnen aus unserer Schwester dem GATACA Systemhaus.	☐

GATACA Empfehlung für erste Richtlinien

Klassifizierung und Kennzeichnung in der Informationssicherheit dienen dazu, Informationen entsprechend ihrer Sensitivität und Bedeutung einzustufen und zu markieren, um sicherzustellen, dass sie entsprechend ihrer Schutzbedürftigkeit behandelt werden. Dies hilft Organisationen, Sicherheitsmaßnahmen gezielt anzuwenden, Zugriffskontrollen zu optimieren und das Risiko von Datenlecks oder -missbrauch zu minimieren.

Mobile Geräte und Remote-Arbeit: Richtlinien für die sichere Nutzung mobiler Geräte und Fernzugriff, einschließlich der Verwendung von VPN und Verschlüsselung.

Richtlinien für den „**Umgang mit Endgeräten**“ sind essenziell, um sicherzustellen, dass alle Geräte, die für Geschäftszwecke verwendet werden, gegen unbefugten Zugriff geschützt sind und Datenverluste vermieden werden. Diese Richtlinien helfen auch, die Einhaltung von Datenschutzstandards zu gewährleisten und das Risiko von Sicherheitsverletzungen zu minimieren.

Richtlinien zur „**Email und Internetnutzung**“ sind wichtig, um die IT-Infrastruktur eines Unternehmens vor schädlichen Inhalten und Cyberangriffen zu schützen und gleichzeitig sicherzustellen, dass die Ressourcen des Unternehmens effizient und für geschäftliche Zwecke genutzt werden. Solche Richtlinien tragen dazu bei, dass Mitarbeiter sich ihrer Verantwortung im Umgang mit Unternehmensinformationen bewusst sind und entsprechend handeln.

Tipps:

Achten sie auf Lesbarkeit. Wir empfehlen Richtlinien, welche sich an alle Mitarbeiter wenden nicht mit Themen anzureichern, welche nur einzelne Fachabteilungen betreffen.

Achten Sie auf Zusammenhänge. Oft Werden Regelungen mehrfach und teilweise wiedersprüchlich in den Regelwerken wiedergegeben. Dies sollte nicht passieren. Vermeiden Sie Doppelungen und achten Sie darauf ob die Zusammenhänge stimmen.

Sollten Sie ein Personal/Betriebsrat haben empfiehlt es sich die Regelungen derart aufzubauen, dass Sie Regelungsaspekte die der Mitbestimmung unterliegen ggf. sepperieren von Regelungsaspekte, welche nicht der Mitbestimmung unterliegen (leichtere Anpassung möglich)

GATACA®
Datenschutz GmbH

Checklisten

Checkliste für Eintritte

	Check
Einrichten des Benutzerkontos: Erstellen von Benutzerkonten und E-Mail-Adressen.	☐
Zugriffsrechte definieren: Festlegen der Zugriffsrechte basierend auf der Rolle und den Aufgabe des neuen Mitarbeiters.	☐
Sicherheitsschulung: Durchführung einer Einführungsschulung zu den Informationssicherheitsrichtlinien des Unternehmens.	☐
Übergabe von Arbeitsmitteln: Bereitstellung und Registrierung von Arbeitsgeräten wie Laptops, Smartphones und Zugangskarten.	☐
Vertraulichkeitserklärung: Unterzeichnung von Vertraulichkeits- und Datenschutzvereinbarungen.	☐

Checkliste für Austritte

	Check
Deaktivierung des Benutzerkontos: Deaktivieren oder Löschen von E-Mail-Adressen und Benutzerkonten.	☐
Rückgabe von Arbeitsmitteln: Sicherstellung, dass alle Unternehmensgeräte und Zugangskarten zurückgegeben werden.	☐
Entfernung von Zugriffsrechten: Entfernen aller Zugriffsrechte auf interne Systeme und Netzwerke.	☐
Datenübertragung und -bereinigung: Übertragung relevanter Arbeitsdateien an Kollegen oder Vorgesetzte und Bereinigung persönlicher Daten.	☐
Abschließendes Exit-Gespräch: Durchführung eines Sicherheits-Exit-Gesprächs, um sicherzustellen, dass der Mitarbeiter alle sicherheitsrelevanten Aspekte versteht und einhält.	☐

Checkliste für Positionswechsel

	Check
Anpassung der Zugriffsrechte: Anpassung der Zugriffsrechte an die neue Position und Entfernung nicht mehr benötigter Berechtigungen.	☐
Aktualisierung von Benutzerkontoinformationen: Aktualisierung der Rollen- und Gruppenzugehörigkeiten in allen Systemen.	☐
Sicherheitsbewertung: Überprüfung der Sicherheitsanforderungen der neuen Position und Anpassung der Sicherheitsmaßnahmen.	☐
Schulung zu neuen Verantwortlichkeiten: Sicherstelle, dass der Mitarbeiter bezüglich der sicherheitsrelevanten Aspekte seiner neuen Rolle geschult wird.	☐
Dokumentation und Compliance-Überprüfung: Aktualisierung der internen Dokumentation und Überprüfung der Compliance-Anforderungen bezüglich der neuen Position.	☐

GATACA© Datenschutz GmbH | Eine Tochter der GATACA© Holding GmbH | seit 2005

Am Riettor 4 | 78048 Villingen-Schwenningen
+49 (0) 7721 / 887979-0
info@gataca.de | www.gataca.de

Geschäftsführer: Moritz Gängel
Handelsregister: HRB 727757 Freiburg
USt-Id-Nr.: DE263703807