ZUSAMMENFASSUNG DER SICHERHEITSMASSNAHMEN BEI HP

Zum Schutz der Kundendaten hält sich HP an eine Reihe solider Informationssicherheitskontrollen, einschließlich Richtlinien, Praktiken, Verfahren und Organisationsstrukturen, um die Vertraulichkeit, Integrität und Verfügbarkeit seiner eigenen Informationen und der seiner Kunden (einschließlich personenbezogener Daten gemäß der Definition in den Kunden- und Datenverarbeitungszusätzen von HP) zu gewährleisten. Im Folgenden finden Sie einen Überblick über die für das gesamte Unternehmen geltenden technischen und organisatorischen Sicherheitsmaßnahmen von HP.

1. Sicherheitsrichtlinie

   HP unterhält weltweit gültige Richtlinien, Standards und Verfahren, die dem Schutz der Daten von HP und seiner Kunden dienen. Zum Schutz der Integrität der Daten und Systeme von HP unterliegen die Einzelheiten in den Sicherheitsrichtlinien von HP der Vertraulichkeit. Dennoch haben wir für Sie im Folgenden die wesentlichen Maßnahmen zusammengefasst.

2. Informationssicherheitsorganisation

   HPs Programm zur Informationssicherheit ist darauf ausgerichtet, die Informationssicherheitsstrategie und -kontrollen des Unternehmens zu steuern und zu pflegen. Mit diesem System werden unternehmensweit die Einhaltung der Sicherheitsrichtlinien und -kontrollen von HP sowie die Einhaltung der Sicherheitsanforderungen seitens seiner Kunden sichergestellt. Das Regelwerk wird jährlich gemäß den branchenüblichen Regelwerken, Gesetzen und Vorschriften zur Cybersicherheit überprüft und der sich entwickelnden Bedrohungslandschaft gegenüber HP angepasst.

3. Risikomanagement bei Cybersicherheit

   HPs Programm zum Risikomanagement bei Cybersicherheit wurde zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationsressourcen entwickelt. Das Programm stellt einen konsistenten Ansatz für die Ermittlung, Bewertung, Priorisierung, Behandlung, Behebung, Verfolgung und Meldung von Cybersicherheitsrisiken bereit. HP definiert seine Risikobereitschaft als die akzeptable Höhe des Verlustrisikos und die Risikotoleranz als den Grad der Abweichung von dieser Bereitschaft. Die Risiken werden mithilfe einer definierten Methodik bewertet, sodass HP das Risiko bei der Informationssicherheit auf ein akzeptables Niveau reduzieren kann. Dieses Programm ist an dem HP Enterprise Risk Management-Prozess ausgerichtet.

4. Personalsicherheit

   Die Personalsicherheitsrichtlinie von HP gewährleistet die Informationssicherheit während der gesamten Betriebszugehörigkeit der Mitarbeitenden durch die Festlegung von Prozessen für den Zutritt zu Einrichtungen sowie den Zugriff auf Informationssysteme und andere Vermögenswerte. Dazu gehört die Einholung schriftlicher Bestätigungen durch Vertraulichkeits- und Offenlegungsvereinbarungen sowie die Durchführung von Hintergrund-Screening-Verfahren. Alle Bewerber/-innen auf eine Anstellung bei HP müssen eine Überprüfung des Hintergrunds in Übereinstimmung mit den einschlägigen Gesetzen, Vorschriften und ethischen Grundsätzen durchlaufen.

5. Bestandsmanagement

   HP verfügt über ein Verfahren zur Identifizierung von technischen Informationsbeständen, zur Kategorisierung kritischer Bestände und zur Aufrechterhaltung dokumentierter Handhabungsverfahren für jede Art von Informationsklassifizierung, einschließlich solcher, die personenbezogene Daten enthalten. Zu diesen Verfahren gehören die Speicherung, Übertragung, Kommunikation, Zugriff, Protokollierung, Speicherung, Zerstörung, Entsorgung, Ereignisverwaltung und Benachrichtigungen gegen Verstöße. Die Sicherheitsrichtlinien und -standards von HP schreiben auch die sichere Entsorgung von Medien vor.

6. Datensicherheit

   HPs Programm zur Datensicherheit beschreibt die zum Schutz der Vertraulichkeit, Authentizität und Integrität von Daten zu implementierenden Sicherheitspraktiken und technischen Kontrollen. Gesetzliche Anforderungen, Wert, Kritikalität und Empfindlichkeit gegenüber unbefugter Offenlegung oder Änderung sind nur einige der Faktoren, die bestimmen, wie Informationen im Rahmen der HP Datensicherheitsrichtlinie klassifiziert werden. Zusätzlich zu den Verfahren für den Umgang mit Daten beschreibt die Richtlinie deren Verschlüsselung, Löschung, Erfassung und Verarbeitung, Aufbewahrung, Sicherung sowie die Vermeidung von Datenverlusten.

7. Zugriffssteuerung

   Für die logische Zugriffskontrolle arbeitet HP nach dem Prinzip der geringsten Privilegien, d. h. der Benutzerzugriff erfolgt über eindeutige Benutzer-IDs und Passwörter. Komplexität, Stärke, Gültigkeit und Kennworthistorie sind in der Kennwortrichtlinie festgelegt. Die Zugriffsrechte werden regelmäßig überprüft und beim Ausscheiden des Personals widerrufen. Vereinbarte Verfahren werden eingeführt, um den Zugang zu Kundensystemen während einer Auftragsdurchführung zu gewähren und zu widerrufen.

8. Kryptografie

   Zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationsbständen wurden von HP eine Reihe robuster Prozesse für die Kryptographie definiert. Zugelassene Protokolle verlangen die Verschlüsselung bestimmter Daten, einschließlich solcher mit personenbezogenen Daten. Unser Programm zur Kryptographie beinhaltet den Einsatz mathematischer Techniken zur Sicherung von Informationen und Kommunikation und stellt sicher, dass nur befugte Parteien auf die Daten zugreifen können. Eine wichtige Komponente von HPs Programm zur Informationssicherheit ist der Schutz von Daten vor unberechtigtem Zugriff und unbefugter Manipulation.

9. Physische und ökologische Sicherheit

   Betriebsgelände von HP sind durch verschiedene physische und elektronische Zugangskontrollen gesichert, darunter Wachpersonal, elektronische Zugangskontrollen und Videoüberwachung (CCTV). Darüber hinaus sind Betriebsgelände mit der notwendigen Infrastruktur ausgestattet, einschließlich Temperaturkontrolle und Stromversorgungssicherheit, die zur Unterstützung kritischer Dienste mithilfe von USV und/oder Dieselgeneratoren gewährleistet wird. Sämtliches HP Personal ist registriert und zum Tragen eines Firmenausweises verpflichtet.

10. Betriebsführung

    HP hat Mindestanforderungen für die technische Infrastruktur festgelegt, einschließlich Workstations, Servern und Netzwerkgeräten. Diese Geräte verwenden vorkonfigurierte Betriebssysteme, wobei die jeweiligen Anforderungen von dem Betriebssystem und den implementierten Steuerungen abhängen. Darüber hinaus hat HP Network Intrusion Detection/Prevention Systems (NIDS/NIPS) im Einsatz, die rund um die Uhr überwacht und verwaltet werden.

11. Kommunikationssicherheit

    Kommunikationssicherheit gewährleistet den Schutz von Informationen innerhalb von Unternehmensnetzwerken. Dazu gehören die Installation und Verwaltung von Netzwerksicherheitskomponenten (z. B. Firewalls), die Trennung von Netzen sowie die Kontrolle von Webfiltern und E-Mail-Bearbeitung. Darüber hinaus umfasst es die Überwachung und Verwaltung von Kommunikationskanälen zur Erkennung und Verhinderung von unberechtigtem Zugriff oder Datenverletzungen.

12. Systemsicherheit

    HPs Richtlinie schreibt eine sichere Entwicklungsmethodik für Systeme und Software während ihres gesamten Lebenszyklus vor. Die Softwareentwicklung besteht aus Initiierung, Entwicklung/Erwerb, Implementierung, Betrieb und Entsorgung. Alle Systemkomponenten werden hinsichtlich ihrer Auswirkung auf die Gesamtsicherheit bewertet. HP hat Kontrollen für Anwendungsdiensttransaktionen eingeführt, darunter die Validierung von Benutzeranmeldedaten, digitale Signaturen, Verschlüsselung, sichere Kommunikationsprotokolle und die Speicherung von Transaktionsdetails innerhalb der entsprechenden Netzwerksicherheitszone. Außerdem werden regelmäßig interne Schwachstellenscans durchgeführt.

13. Dritte und Subunternehmen

    HP hat Verfahren zur Auswahl von Subunternehmern vor, die umfassende vertragliche Sicherheitsanforderungen erfüllen. Bei relevanten Lieferanten, die Daten von HP oder Kunden verarbeiten oder auf das HP Netzwerk zugreifen, führt HP Cybersecurity zur Überprüfung eines Informationssicherheitsprogramms mit physischen, technischen und administrativen Schutzmaßnahmen regelmäßig eine Risikobewertung durch. Diese Bewertung hat zu erfolgen, bevor der Lieferant auf HP Informationen zugreifen darf.

14. Umgang mit Informationssicherheitsvorfällen

    HP hat einen umfassenden Prozess für den Umgang mit Cybervorfällen implementiert, in dem Zweck, Umfang, Rollen, Zuständigkeiten, Involvierung des Managements, organisatorische Koordination, Implementierungsverfahren und die Überprüfung der Einhaltung von Vorschriften festgelegt sind. Dieser Prozess wird jährlich überprüft und aktualisiert. Das Cyber Incident Response Team, zu dem auch in Incident Response und Krisenmanagement geschulte Mitarbeitende von HP Cybersecurity gehören, führt regelmäßig Table-Top-Überprüfungen des Prozesses und aller Vorfälle oder Ereignisse durch.

15. Business Continuity-Verwaltung

    HPs globale Programm zur Continuity of Operations gewährleistet End-to-End-Kontinuität durch gemeinsame, standardisierte und dokumentierte Planungsprozesse. Das Unternehmen überprüft regelmäßig seine Pläne zur Business Continuity, um deren Wirksamkeit sicherzustellen, und testet und aktualisiert alle Pläne mindestens einmal jährlich. Darüber hinaus werden alle in den Business Continuity Plan involvierten Mitarbeitenden entsprechend geschult.

16. Compliance

    Compliance ist ein wichtiger Ansatz, den HP zur Erfüllung der gesetzlichen, vertraglichen und internen Anforderungen an ein effektives Informationssicherheitsprogramm verfolgt. Regelmäßige Überprüfungen der Informationssicherheit stellen sicher, dass die Protokolle in die Arbeitsabläufe der einzelnen Unternehmensgruppen integriert sind. Der Überprüfungsprozess sorgt auch dafür, dass die Dokumente auf dem neuesten Stand gehalten werden und sie bei einer Änderung der Anforderungen die aktuellen gesetzlichen Verpflichtungen enthalten.

17. Payment Card Industry

    Das Regelwerk der Payment Card Industry (PCI) ist ausschlaggebend für HPs Ansatz zur Erreichung der PCI-Compliance, wobei es die Verantwortlichkeiten des Unternehmens und die Sicherheitskontrollen im Einklang mit dem PCI DSS beschreibt. Durch die Installation und Wartung von Netzwerksicherheitssteuerungen wie Firewalls stellt HP sicher, dass die PCI-Anforderungen erfüllt werden.

18. HP Produktsicherheit

    HP Produktsicherheit legt die wichtigsten Verfahren zur Sicherung von HP Produkten, wie z. B. Code Signing, Management von Sicherheitslücken in Produkten, Herausgabe von Sicherheitsbulletins und Meldung von Produktsicherheitsproblemen. Diese Maßnahmen sorgen dafür, dass HP Produkte sicher und zuverlässig für die Benutzer bleiben. Produktsicherheit ist bei HP von größter Bedeutung, da sie dazu beiträgt, das Vertrauen der Kunden zu erhalten und vor potenziellen Bedrohungen zu schützen.

19. HP Dienstsicherheit

HP Dienstsicherheit legt die wichtigsten Verfahren zur Sicherung der für HP Kunden angebotenen Dienste. Diese Richtlinie befasst sich mit verschiedenen Bereichen der Dienstsicherheit, einschließlich mit HP Infrastruktur betriebener, von Drittanbietern gehosteter, von Partnern gehosteter Umgebungen und von Kunden gehosteter Umgebungen. Diese Maßnahmen stellen sicher, dass HP Dienste für die Benutzer sicher und zuverlässig bleiben. Durch die Implementierung stabiler Sicherheitsverfahren gewährleistet HP die Sicherheit sowie Integrität seiner Produkte und Dienste, um für eine sichere, vertrauenswürdige Umgebung für alle Benutzer zu sorgen.