

HP PrintOS – Sicherheit und Verfügbarkeit



Inhaltsverzeichnis

Einführung.....	2
Sicherheitsarchitektur-Diagramm	2
Sicherheit	3
Sichere und hochverfügbare Rechenzentren	3
Compliance-Framework.....	3
Sichere Kommunikation und Datenschutz.....	3
Sicheres Account-Management und Zugriffsprüfung	3
Datenschutz	3
Disaster Recovery und Datensicherung.....	4
Sicherheitsüberwachung und Sicherheitsmanagement	4
Safe Harbor und Binding Corporate Rules	4
Verfügbarkeit	4
Zusammenfassung.....	4

HP PrintOS ist ein Druckproduktions-Betriebssystem mit einer Reihe mobiler und webbasierter Apps, die Ihre Produktion vereinfachen und automatisieren – damit Sie noch mehr aus Ihren HP Grafikdruckern und Druckmaschinen herausholen können. Nutzen Sie diese Lösung, um Ihren Druckbetrieb immer weiter zu optimieren, Ihre Mitarbeiter zu begeistern und bessere, schnellere Entscheidungen zu treffen. Mithilfe von PrintOS können Sie so viele Jobs verwalten, wie Sie möchten – von der Job-Eingabe bis hin zur Auslieferung. PrintOS ermöglicht es Ihnen, optimal mit Partnern und Kollegen zusammenzuarbeiten und sich neue Wachstumschancen zu erschließen. Dabei können Sie jederzeit und überall auf die offene und sichere, cloudbasierte PrintOS-Plattform zugreifen.

HP stellt ein Höchstmaß an Datenschutz in der Cloud sicher. Dieses Dokument befasst sich mit der Sicherheit und Verfügbarkeit unserer PrintOS-Lösung. Erfahren Sie, welche Maßnahmen HP ergreift, um Ihren Anforderungen in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gerecht zu werden.

Rechenzentren

(ISO-27001-Zertifizierung & Serviceanbieter der Ebene 1
gemäß Payment Card Industry (PCI) Data Security Standard (DSS).)

Die Rechenzentren werden jährlichen SOC-1-Audits unterzogen und wurden erfolgreich für Systeme des US Federal Government auf der Stufe „moderat“ sowie für DoD-Systeme (US-Verteidigungsministerium) auf der DIACAP-Ebene 2 eingestuft.



Data Warehouse

Ruhende Daten werden in einem verschlüsselten Dateisystem mithilfe von LUKS mit einer 1024-Bit-Verschlüsselung oder AES 256 gespeichert. Passwörter werden mit einem Salt versehen und mit dem Hashverfahren SHA-256 verschlüsselt.



IMPACT Big Data



Firewall und private Subnetze verhindern ungewollte Zugriffe auf unsere Umgebungen.



Datenübertragungen erfolgen über TLS 1.2-Verbindung.



PrintOS

Der Zugriff auf Daten ist durch Authentifizierung, Autorisierung, Account-Management und Audit-Protokollierung geschützt.

Auf die Druckmaschine bezogene Anwendungen



Substrate Manager



PrintBeat



Events on Cloud

Auf das DFE bezogene Anwendungen



Resource Manager



Site Flow



Box



Composer



Imposer

Die Übertragung aus Data Warehouses erfolgt über TLS 1.2-Verbindung.

Kundennetzwerk/-Firewall



HP Druckmaschine/Drucker



HP DFE/RIP



Kunden-PC



Tablet



Smartphone

Sicherheit

Zum Schutz Ihrer Informationen setzt HP auf höchste Sicherheitsstandards. Wenn Daten an die PrintOS-Cloud-Plattform übertragen werden, haben Sie als Benutzer die Gewissheit, dass HP alles tut, um diese Daten zuverlässig zu schützen. Um den wachsenden Herausforderungen einer modernen Cloud-Umgebung gerecht zu werden, überwacht und verbessert HP konstant die Anwendungen, Systeme und Prozesse, die für HP PrintOS entscheidend sind.

Von sicheren, hochverfügbaren Rechenzentren bis hin zu strenger Sicherheitsüberwachung und zuverlässigem Datenmanagement: HP nutzt einen mehrschichtigen Ansatz, um Ihre Informationen und Ihr Unternehmen zu schützen.

Sichere und hochverfügbare Rechenzentren

Die Sicherheitsstrategie von HP konzentriert sich vor allem auf die Rechenzentren, die Ihre Informationen speichern. Zwar können Sie die Rechenzentren, die HP für die PrintOS-Plattform verwendet, nicht persönlich besuchen, aber unser Sicherheitsüberprüfungsprozess gewährleistet, dass alle Standorte durch externe Spezialisten überprüft und zertifiziert werden. Unsere Rechenzentren haben die ISO-27001-Zertifizierung erhalten und sind gemäß dem Payment Card Industry (PCI) Data Security Standard (DSS) als Serviceanbieter der Ebene 1 validiert. Darüber hinaus werden die Rechenzentren jährlichen SOC-1-Audits unterzogen. Sie wurden erfolgreich für Systeme des US Federal Government auf der Stufe „moderat“ eingestuft – außerdem für DoD-Systeme (US-Verteidigungsministerium) auf DIACAP-Ebene 2. Die Rechenzentren sind rund um die Uhr durch geschulte Sicherheitsmitarbeiter besetzt; und der Zugriff wird streng gemäß dem Prinzip der minimalen Rechte autorisiert.

Compliance-Framework

Die Einhaltung globaler Standards durch HP macht es für Sie leicht, nationalen und regionalen Anforderungen gerecht zu werden. HP pflegt ein dynamisches Compliance-Framework. Das bedeutet: Die sich ständig weiterentwickelnden Normen und Bestimmungen werden permanent verfolgt und, wenn möglich, sogar vorweggenommen. Das PrintOS-Compliance-Framework wurde konzipiert, um unterschiedlichste Zertifizierungen, gesetzliche Vorschriften und Prüfanforderungen Dritter konsistent zu erfüllen.

Sichere Kommunikation und Datenschutz

HP setzt auf unterschiedliche Maßnahmen, um bestmöglichen Datenschutz zu gewährleisten. Daten werden bei der Übertragung durch eine TLS-1.2-Verbindung gesichert. Ruhende Daten werden in einem verschlüsselten Dateisystem mithilfe von LUKS mit 1024-Bit- oder AES-256-Verschlüsselung gespeichert. Passwörter werden mit einem Salt versehen und anschließend mit dem Hashverfahren SHA-256 verschlüsselt. Die PrintOS-Plattform wird einem umfangreichen Sicherheitsüberprüfungsprozess unterzogen, der eine Sicherheitsarchitektur-Checkliste, eine Code-Prüfung durch Experten und Schwachstellen-Fuzzing umfasst.

Sicheres Account-Management und Zugriffsprüfung

Der Zugriff auf Ihre Daten ist durch Authentifizierung, Autorisierung, Account-Management und Audit-Protokollierung geschützt. Diese Faktoren werden im Rahmen des Prüfungsprozesses für die Sicherheitsarchitektur bewertet.

HP führt detaillierte Audit-Protokolle, die Datenelemente wie Account-Namen, Datum und Zeitstempel sowie ausgeführte Aktivitäten aufzeichnen. Der Datenbankzugriff ist auf autorisierte Mitarbeiter beschränkt. Audit-Protokolle werden regelmäßig gesichert und gepflegt.

Datenschutz

HP hat eine Datenschutzerklärung ausgearbeitet und veröffentlicht, die den Verkauf, die Vermietung und jegliche andere Form der Weitergabe persönlicher Daten an Dritte streng untersagt. Die globalen Datenschutzstandards von HP sind auf der PrintOS-Website oder unter hp.com/go/privacy abrufbar.

HP verlangt und bietet Sicherheits- und Datenschutzs Schulungen für alle HP Mitarbeiter, die mit vertraulichen oder persönlichen Informationen umgehen. Auch die Standards und Prozesse in Bezug auf globale personenbezogene Daten (PII) hält HP gewissenhaft ein.

Um die Vertraulichkeit Ihrer Daten zu garantieren, kommen zudem vielfältige administrative, technische und physikalische Schutzmaßnahmen für Kundenumgebungen zum Einsatz – ebenso wie einschlägige Branchenprogramme (etwa Safe Harbor, ISO u. a.).

Disaster Recovery und Datensicherung

Informationen sind ein wertvolles Gut, das jederzeit verfügbar sein muss. PrintOS basiert auf einem branchenführenden Cloud-Design, das auf jeder Ebene physische und logische Redundanz bietet. Jede Virtualisierungsebene ist redundant, um hohe Verfügbarkeit und Skalierbarkeit sicherzustellen.

Sicherheitsüberwachung und Sicherheitsmanagement

Wir sorgen dafür, dass Ihre Informationen nicht in falsche Hände geraten. Firewall und vertrauliche Subnetze verhindern ungewollte Zugriffe auf unsere Umgebungen; und unsere Angriffserkennungssysteme arbeiten rund um die Uhr, damit ein Höchstmaß an Schutz für Kundendaten gewährleistet ist. Darüber hinaus überprüft HP die Umgebung regelmäßig auf Sicherheitslücken im Bereich der Anwendungen und der Infrastruktur. Bei Vorfällen schaltet sich unser Reaktionsteam blitzschnell ein, um Probleme umgehend zu beseitigen.

Safe Harbor und Binding Corporate Rules

HP erfüllt die Rahmenbestimmungen des Safe Harbor für USA – EU sowie für USA – Schweiz, gemäß den Vorschriften des US-Handelsministeriums in Bezug auf die Sammlung, Verwendung und Archivierung persönlicher Daten aus Ländern der Europäischen Union und der Schweiz. Dabei hat sich HP zur Einhaltung der Safe-Harbor-Prinzipien in Bezug auf folgende Punkte verpflichtet: Informationspflicht, Wahlmöglichkeit, Weitergabe, Sicherheit, Datenintegrität, Zugriff und Vollzug. Mehr Informationen über das Programm „Safe Harbor“ sowie die Zertifizierung von HP finden Sie unter export.gov/safeharbor/

HP hat außerdem Binding Corporate Rules (BCR) eingeführt, die durch alle Datenschutz-Regulierungsbehörden im europäischen Wirtschaftsraum (EWR) und in der Schweiz mit Wirkung zum Juni 2011 genehmigt wurden. Diese BCR stellen sicher, dass die persönlichen Daten von abgedeckten Einzelpersonen aus dem EWR während der Verarbeitung durch globale HP Zweigstellen angemessen geschützt werden.

Verfügbarkeit

Ihr Unternehmenserfolg und der Schutz Ihrer Informationen sind ein zentrales Anliegen von HP. Deshalb ist die Site-Verfügbarkeit für die PrintOS-Cloud-Plattform nie geringer als 99,9 %.

Wie bei allen Software-as-a-Service-Anwendungen (SaaS) plant HP zeitweise Ausfallzeiten für Wartungszwecke oder das kundenorientierte Verbessern, Hinzufügen oder Entfernen von Eigenschaften und Funktionen ein. Solche geplanten Ausfallzeiten werden nicht in die Verfügbarkeitsberechnung der PrintOS-Lösung einbezogen.

Ausfälle aus Gründen, für die HP keine Verantwortung trägt, fließen ebenfalls nicht in die Kalkulation der PrintOS-Verfügbarkeitsquote ein. Zu diesen Ausnahmen zählen u. a. der Ausfall von Computer-Infrastruktursystemen an der Betriebsstätte eines Kunden oder Fehler bei der Übertragung von Informationen aufgrund von höherer Gewalt, Regierungshandlungen, Hochwasser, Feuer, Erdbeben, politischen Unruhen, Terroranschlägen, Streiks oder ähnlichen Arbeitsunterbrechungen.

HP bemüht sich im wirtschaftlich angemessenen Rahmen, alle geplanten Ausfallzeiten präzise zu terminieren und die Kunden entsprechend zu informieren.

Zusammenfassung

So wie die Cloud neue Möglichkeiten zur Bereitstellung und Nutzung innovativer Technologien schafft, revolutioniert auch HP PrintOS die Art und Weise, wie Druckdienstleister jeder Größe ihre Unternehmen führen und Gewinne erwirtschaften können. Unsere Lösung gewährleistet auf vielen verschiedenen Ebenen, dass Ihre Daten und Systeme sicher sind, wenn Sie HP PrintOS verwenden. Mit Vertraulichkeit, Datenschutz und Verfügbarkeit als Kern unserer Sicherheitsstrategie können Sie HP und der PrintOS-Plattform fest vertrauen, wenn es um den Schutz Ihrer Informationen und Ihres Unternehmens geht.

Weitere Informationen finden Sie unter

hp.com/go/printos

Für Updates anmelden

hp.com/go/getupdated



Mit Kollegen teilen

