Security and Compliance Whitepaper

1.1 Purpose

This white paper discusses various security aspects of EveryonePrint products in the following parts:

- Shared security responsibilities
- Security compliance and privacy
- HCP compliance
- HCP security architecture
- Security features of EveryonePrint products
- HCP security ecosystem

This white paper also provides the best practice for the secure use of the HCP service. Allowing customers to make better use of their print service and to provide insight into the overall security options within the HCP environment.

1.2 EveryonePrint Cloud Security Mission

EveryonePrint's cloud security mission is to protect the integrity, confidentiality, and availability of our customers', partners' and internal data. EveryonePrint is committed to being transparent about security practices which helps customers and partners understand our approach

Contents

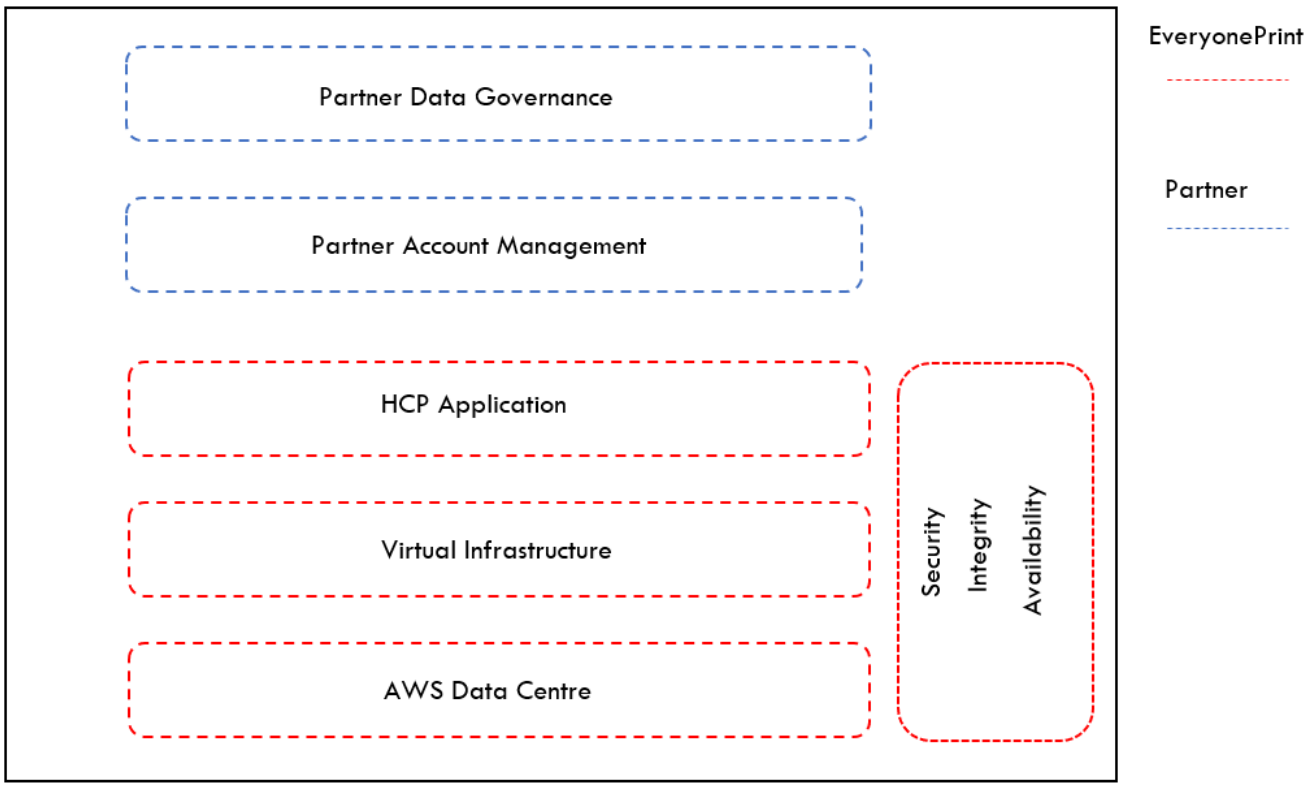
1.3 The Shared Security Responsibilities

EveryonePrint and its Partners are jointly responsible for the security of their customers' print infrastructure. HCP can be hosted either by EveryonePrint A/S, by a Partner (within a Data Centre selected by Partner) or by the Customer.

1.3.1 Hosted by EveryonePrint

EveryonePrint is responsible for the security of the underlying cloud service platform, network connectivity of the application, and physical data centres, and partners are responsible for the user management, account management and data governance and rights management.

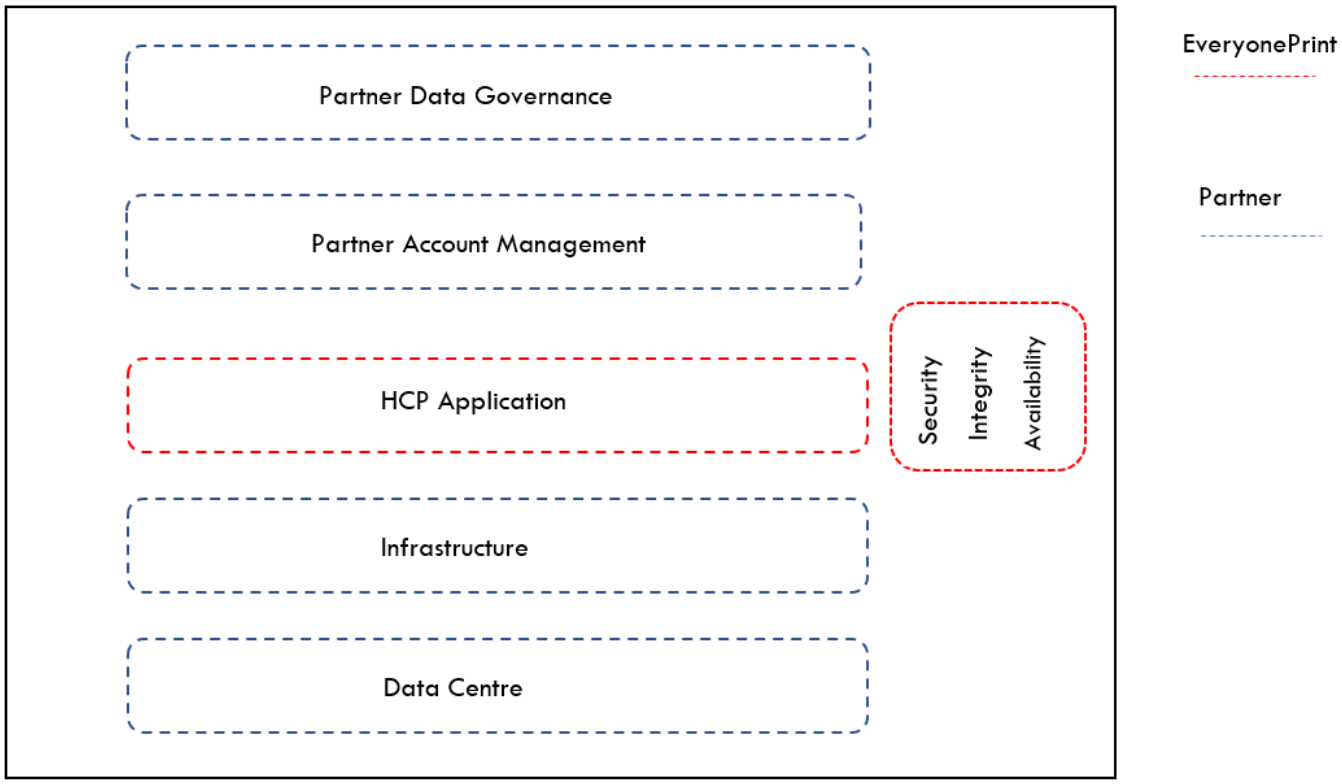
The shared security responsibility model is somewhat different than the typical security model a customer would see in an on-premise print environment. By using EveryonePrint's Cloud infrastructure, customers can leverage the underlying security, integrity & availability that HCP provides, attaining a higher level of security relative to the investment required when managing the environment themselves.



1.3.2 Hosted by Partner / Customer

EveryonePrint is responsible for the security of the underlying application and partners are responsible for the user management, account management, data governance, infrastructure and data centre.

Virtua
l



EveryonePrint HCP offers various security features and services to help protect customers' print infrastructure. In turn, partners must configure and use HCP service as intended.
With security responsibilities shared between EveryonePrint and its partner, HCP can provide a secure print service to help meet the security needs of customers, thus relieving much of the underlying security burdens while allowing the customer to focus more on their core business needs.

1.4 Security Responsibilities of HCP

In general, HCP is responsible for the security of its Virtual infrastructure, OS, and cloud services/products, and provides customers with the technical means necessary to protect their print service

EveryonePrint ensures the cloud platform security by:

- Protecting the physical security of cloud data centres by outsourcing this to best in class vendors such as AWS.
- Protecting the security of software, and network of the cloud platform by means of OS- and database-patch management, network access control, Anti-DDoS, and disaster recovery, etc.;
- Identifying and fixing security vulnerabilities of the Application or HCP Cloud service in a timely manner without affecting partners / customers ' service availability;
- Cooperating with independent third-party security regulation to evaluate security and compliance of EveryonePrint cloud service security

1.4.1 Security Responsibility for Partners/Customers

EveryonePrint Partners (Data Controller), are required to meet strict safety and security demands, and these requirements naturally involve handling documents through HCP. We see this as an opportunity and take on a

proactive approach to fulfilling our duties, thereby helping you fulfil yours. This section describes individual actions that foster data security during the HCP lifecycle:

- In EveryonePrint-hosted solutions, data is hosted by major third parties, who have a contractual obligation with us, ensuring they handle data according to GDPR-requirements.
- EveryonePrint and partners will never use personal data for any other purposes than delivering the HCP service. Further, it is ensured that any present and future sub-suppliers uphold GDPR. For example, this means all data is stored on servers within EU/EEA, unless otherwise explicitly agreed upon.
- The customer/Partner -appointed administrator may however choose to retain the document in HCP for a predefined number of minutes/hours hereafter – for example to enable re-print. This will not impose a major security risk, other than more data is available in case of a breach

1.5 Security Compliance and Privacy

EveryonePrint adheres to domestic and international information security standards, as well as industry requirements. We integrate compliance requirements and standards into our internal control framework and implement such requirements and standards by design in our cloud print service. We are also engaging with independent third parties to verify the compliance of EveryonePrint according to various requirements. Our framework and compliance foundations are based on the following:

1.5.1 ISO27001:2013

EveryonePrint has been ISO27001 certified. It is a security management standard that specifies the security management best practices and comprehensive security controls. The basis of this certification is the development and implementation of rigorous security program which includes the development and implementation of Information security management system (ISMS) which defines how EveryonePrint manages the information security in a holistic manner.

- EveryonePrint has developed information security policy that considers the impact, threats and vulnerabilities of all of our assets
- EveryonePrint has robust framework developed for managing the data protection both at rest as well as in transit
- EveryonePrint has a framework to train all its employees on information security based on ISO27001

1.5.2 SOC2

Soc2 is a security management standard that describes the controls relevant to security, availability, process integrity, confidentiality. EveryonePrint has developed a framework that considers this information security standard. Products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to ensure the highest level of security, and ensure the trust of our customers. We're constantly working to expand our coverage against global IT best practices.

1.5.3 Transparency

EveryonePrint will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends EveryonePrint a demand for Customer Data, EveryonePrint will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, EveryonePrint may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then EveryonePrint will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless EveryonePrint is legally prohibited from doing so.

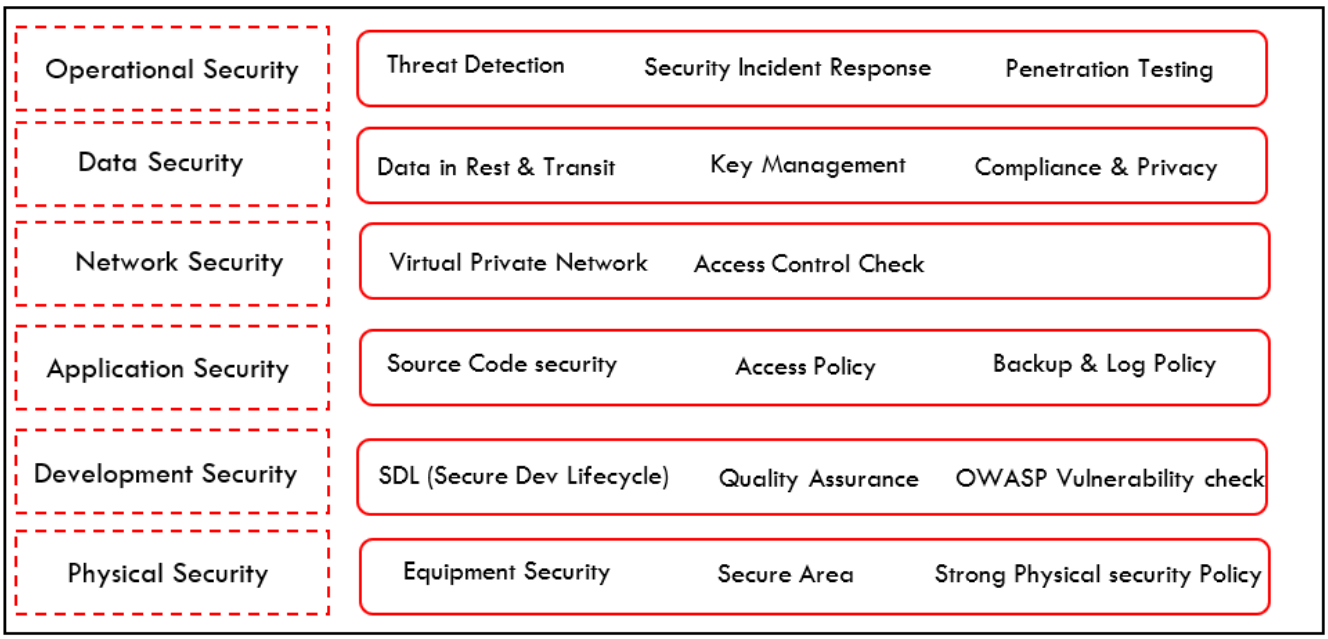
1.6 HCP Global Infrastructure

EveryonePrint HCP offers high availability, secure, and reliable cloud computing infrastructure by: setting up access to cloud data centres across multiple regions and zones globally; delivering a better network access experience providing print service with high availability infrastructure and multi-replica data redundancy; upgrading products and fixing vulnerabilities using the patching technology; and ensuring operation security while achieving compliance.
Everyone Print HCP data centre resources are deployed across multiple regions worldwide, Customer businesses can be deployed across regions and zones to implement a high availability architecture

Country	Region
Ireland	EU(Ireland)
United Kingdom	United Kingdom
US	US East (N.Virgina)
Singapore	Asia Pacific (Singapore)

1.7 HCP Cloud Security Architecture

This section provides an overview of the overall security architecture and describes the key features of each architecture layer by briefly covering it.



1.7.1 Physical Security

1.7.1.1 Equipment Security

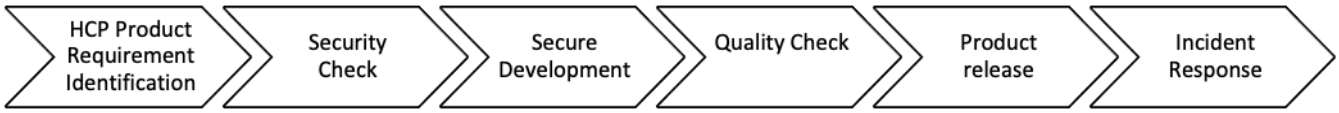
EveryonePrint outsources hosting of its platform infrastructure to leading cloud infrastructure hosting providers, currently Amazon Web Services, who in turn provide high levels of physical and network security and maintain various levels of audited security, including SOC 2 Type II and ISO 27001 compliance. Please see AWS audit reports for additional information about physical environments. https://aws.amazon.com/compliance/data-center/data-centers/

1.7.1.2 Secure Area

EveryonePrint's Headquarters is secured with access controls. EveryonePrint employees in HQ have specific access keys to enter the HQ. All the visitors to EveryonePrint HQ are accompanied by an employee inside the premises. CC TV and image capturing facilities are installed in the building to secure the physical areas.

1.7.2 Development Security

The EveryonePrint secure development lifecycle (SDL) introduces security and privacy considerations throughout all phases of the development process, helping our developers; build highly secure software; address security compliance requirements; and reduce development costs. The guidance, best practices, tools, and processes in our (SDL) are practices implemented to build more secure products and services has been certified according to SD PAC by Security Innovation Inc.



The 6 phases above indicate how the secure development is conducted to build EveryonePrint products and services;

- Product requirement stage is when the business requirement is noted down in our development tool and inform all the stakeholders on the baseline
- Security check is the phase where the security architecture of the product is reviewed based on the baselining, privacy and compliance requirement
- Once the security check is conducted the developers of the EveryonePrint in accordance with the security requirements achieve the relevant security features and goals of the product
- Quality check is the phase where the EveryonePrint QA team reviews on the architecture, design, and application environment of the product according to the security requirements, and performs code review
- Product release is the phase where the changes approved by the EveryonePrint Change Authority and the product is released to the market
- Incident response is the phase where the incidence response team quickly rates it and determines its priority and schedule for a fixing. The incidence response team ensures allocation of resources to efficiently and effectively fix vulnerabilities to guarantee the security. In all these phases the development security check is conducted based on the OWASP security principle

1.7.3 Application security

1.7.3.1 Source Code Security

In the secure product lifecycle (SPLC) of print solutions, the EveryonePrint team strictly review and validate the source code security to ensure a high level of code security for all our development.

1.7.3.2 Access Policy

EveryonePrint follow the principle of least privilege, organizational responsibility is divided amongst organization and specific roles are created to manage those responsibilities. Proper governance is maintained to regulate the roles and access provided to the roles.

1.7.3.3 Backup & Log Policy

Before important operations such as OS replacement, upgrading application software or migrating business data, necessary back up is taken. EveryonePrint follows set standards for change management and performs regular backups on a daily basis. Necessary logs are maintained to track the user operation and health check of instances.

1.7.4 Network Security

EveryonePrint HCP solution is designed in such a way that network isolation of production networks from non-production networks is maintained. Direct access is forbidden from a non-production network to any servers and network devices in a production network

Using AWS state of the art technology we have configured to forbid access from cloud service networks to physical networks. EveryonePrint also takes network control measures to prevent unauthorized devices from connecting to the internal network of the HCP platform and to prevent the servers of the internal platform from connecting to external devices

1.7.5 Data Security

EveryonePrint restrict its personnel from accessing Customer Data without authorization by EveryonePrint Management and without a reasonable cause. EveryonePrint have established appropriate contractual obligations upon its personnel, regarding confidentiality, data protection and data security

1.7.5.1 Data in Rest & Transit

EveryonePrint enables HTTPS encryption within HCP to ensure data transmission security. HCP uses HTTPS encryption for data transmission. HCP uses industry standard SSL/TLS protocol. Key Management Service (KMS) for key management and data encryption capabilities are used to manage the user data at rest.

EveryonePrint classifies all the data falling into its processing scope. There is a clear bifurcation of all user data stored in the infrastructure. When customers leave the HCP service, EveryonePrint follows strict standards for eliminating the data of the customer.

1.7.5.2 General Data Protection Regulation - GDPR (EU)2016/679

Unless otherwise agreed between EveryonePrint and the Customer prior to account setup, all processing and storage of Customer Data within the HCP solution will be handled by default in the customer contracting region. Accordingly, customers who order within the EU will by default have their data stored in the EU. US customers by default in US datacenter, APAC in AP and UK government customers in UK gov cloud.

1.7.6 Operational Security

Once a security vulnerability is detected, the incident response team quickly rates it and determines its priority and schedule for a fix to be provided.

1.7.6.1 Penetration Testing

EveryonePrint performs a vulnerability assessment of its application on a quarterly basis. Results of these test are analysed by EveryonePrint security team, triaged, prioritized and necessary remediation procedures are conducted in a timely manner. We also have an additional layer of security provided by our cloud vendor against DDOS and external intrusions.
Our Partners are welcome to perform either security controls assessments or penetration testing on EveryonePrint's HCP environment.
Please visit our website to get more details on how to request penetration testing.

1.8 Version History

November 2021 - Version 1.1

Note - This document does not create any warranties, representations, contractual commitments, conditions from EveryonePrint, its affiliates, suppliers or licensors. The responsibilities and liabilities of EveryonePrint to its customers are controlled by contractual agreements, and this document is not part of, nor does it modify, any agreement between EveryonePrint and its partners or customers.