Cloud Security Principles

Martin Bradburn
PEA SOUP HOSTING LIMITED | WELLINGTON WAY, BROOKLANDS BUSINESS PARK,
WEYBRIDGE, SURREY, KT13 0TT

Document information

Important Notice

This document has been prepared by PeaSoup Hosting for the sole use of PeaSoup Hosting and its recipient. The contents are confidential and must not be communicated in whole or in part to any other party without the prior written approval of PeaSoup Hosting.

PeaSoup Hosting has prepared this document in good faith based on the information made available to it. Many factors outside PeaSoup Hosting current knowledge or control may affect the recipient's needs and plans. The statements in this document are qualified accordingly.

This document is provided subject to contract. Nothing in this document nor in any related discussions or correspondence shall be construed as an offer, nor the basis of any contract, nor may a representation which may be relied upon by any person except as PeaSoup Hosting expressly agree in writing.

The following notice applies to this document and shall be reproduced on any permitted copies.

Change history

Version	Date	Author	Notes
1.0	3rd Oct 2018	M Bradburn	Initial Document
1.1	16th Oct 2018	M Bradburn	Refine comments

Contents

1 Introduction

PeaSoup Hosting provide cloud services that can help address the security, compliance and flexibility needs of modern organisations. In addition, PeaSoup work with customers to understand their assurance concerns, and to help define their responsibilities regarding protecting data and environmental infrastructure after services are provisioned.

PeaSoup delivers infrastructure as a service, providing a complete virtual datacentre (vDC)with all the capabilities of a physical datacentre, a platform to host virtual servers and to deliver applications dedicated to each customer rather than providing common shared services.

As the name suggests, Infrastructure as a Service (IaaS) provides Infrastructure. The platform and application stack built on top of the service architecture is the responsibility of each customer. Along with the responsibility for designing and building these systems comes the need to ensure they are properly protected. In practice, this entails securely configuring the infrastructure and anything built upon it.

To improve the underlying security of the UK internet and to protect critical services from cyber-attacks, the National Cyber Security Centre was set up, the information security arm of the Government Communications Headquarters (GCHQ), and provides a framework built around 14 Cloud Security Principles. These Cloud Security Principles are expansive and thorough and include such important considerations as data in-transit protection, supply chain security, identity and authentication and secure use of the service.

The cloud security principles are a guidance that should be used when considering a cloud service to identify any potential risks and requirements.

Further details can be found on the NCSC's website:
https://www.ncsc.gov.uk/guidance/introduction-understanding-cloud-security

This document provides an insight into how PeaSoup's services align with the fourteen cloud security principles set forth in the CESG/NCSC publication "Implementing the Cloud Security Principles," this can assist organisations to fast-track their ability to meet their compliance obligations using PeaSoup cloud-based services in the UK.

2 The UK Governments 14 Cloud Security Principles

In its publication "Cloud Security Guidance: Summary of Cloud Security Principles," CESG/NCSC, laid out 14 security principles that organisations should use when evaluating cloud services, and that cloud service providers should consider when offering those services to government customers (referred to as "consumers" in the principles). The 14 principles are aligned with ISO 27001, an auditable, international, information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally defines requirements for a complete ISMS to help protect and secure an organisation's data.

The principles defined by CESG/NCSC are:

2.1 Data in transit protection

Data in transit protection *- Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.*

Data in transit can be protected using a private circuit, terminating directly into the edge of the virtual Datacentre, this connecting the cloud in the same manner as another office, participating on the same WAN topology. Direct connections can be cross connected to PeaSoup from either the CenturyLink datacentre in Goswell road, London or through the Telehouse North or Telehouse Metro datacentres.
This direct connection can apply to other community networks, providing the consumer holds the relevant certifications of connection with VLAN or more appropriately VXLan protection through to PeaSoup.

For public networks, configurable from the PeaSoup Cloud, an edge security device provides IPsec VPN capabilities and provides secure site-to-site connectivity using widely supported standards such as Internet Key Exchange (IKE) with 256-bit Advanced Encryption Standard (AES-256) for strong encryption. This capability enables you to interconnect virtual Datacentres securely to other firewalls from a variety of vendors. Additionally, an SSL connection can be made available for end devices with either third party or self-signed certificates.

These features are part of the overall edge security capabilities. Firewalls are tightly integrated into the PeaSoup cloud whereas you can use the firewall-rule table to directly select objects such as workloads, port groups and virtual networks. This integration makes rule creation faster and less error prone. Once defined, rules can be enforced at either the perimeter of the virtual Datacentre, or directly in front of a workload at the vNIC level to perform stateful packet inspection with improved performance and low latency.

When accessing to the PeaSoup cloud management portal the data transmitted between the portal and the administrator's device is sent over an encrypted TLS channel.

2.2 Asset Protection and Resilience

Asset Protection and Resilience - *Consumer data, and the assets that store or process such data, should be protected against physical tampering, loss, damage, and seizure.*

All data in the PeaSoup cloud is stored in the UK, at all times. The primary site is a Tier 3 datacentre in London, operational 24x7x365. The secondary site, planned for January 2019, is again specified to have full resilience and security to a Tier 3 level by the standards defined by the Telecommunications Industry Association with the latest publication of ANSI/TIA-942. PeaSoup also ensure that in line with our security polices, the datacentres must have current BSI certifications to ISO 27001:2013, information Security Management System certificate and ideally ISO 22301:2012 Business Continuity Management System certificate and an ISO 9001 (Quality Management System) certifications to satisfy the requirements of PCI DSS Payment card industry.
As a data processor under GDPR compliance, PeaSoup place a restriction of data movement outside of UK borders. On explicit instruction data can be transferred to other EU countries or none EU member states providing the conditions of Article 44 of the GDPR (Regulation (EU) 2016/679) have been fulfilled.

The main PeaSoup physical servers are located and protected in line with the GDPR Article 32 for Confidentiality, Integrity, availability and resilience. They are located in a data suite, certified to a PCI-DSS service provider level, with full monitored CCTV, which is locked using magnetic tags that are issued only to authorised personnel. The data suite is part of the building that has both magnetic key entry and number pad control, accessed only by coming through an airlock which is manned 24/7 by security guards and CCTV, checking photo ID against prior arrangement of the visit. The main doors are also protected by magnetic key and number pad entry with the remaining borders protected with razor wire and high fences. All data and servers that deliver the

PeaSoup cloud vDC's are backed up daily to a separate infrastructure in a full controlled and encrypted manner with off-site copies to protect against failure in line with the PeaSoup disaster recovery processes. Some customer services are also protected in the same manner, at the request of the customer to replicate their system to a second location.

2.3 Separation Between Consumers

Separation Between Consumers *- Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another. If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.*

Each consumer resides within their own virtual Datacentre (vDC). This creates a complete separation as each vDC has its own networking, firewalls and users. Management access to the vDC is controlled based on authentication and only provides visibility to the vDC, there is no access to any other part of the PeaSoup cluster. Each vDC has a limited bandwidth resource meaning in the event of a DDoS attack, no other users of the service will be affected. This and other network abstraction techniques separate the different consumers from each other. Network traffic in each vDC in a pool is isolated at layer 2 from all other networks. Finally, and most importantly protection from noise is assured to the consumers through the reservation of processing and memory resources set in those abstractions.

2.4 Governance framework

Governance framework *- The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.*

PeaSoup have a security governance framework with a Security Officer at board level whom is responsible for the compliance to our information security as outlined in our policies.
The PeaSoup policies were developed and periodically checked with an external security agency combining the controls from ISO27001, CSA Cloud Controls Matrix and PCI-DSS service provider certifications. In addition to the information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction. These are supplemented with our Information Classification & Handling, Access Control and Authentication, Business Continuity, Infrastructure Management, Risk Management, Change Control, Remote Access, Supplier Security, Physical and Environmental Security, Incident Management, Security Incident Management Procedure, Encryption Key Management, Back-Up and Document & Record Control Policies.
All policies and controls in place are in line with current data protection legislation meaning any and all laws, statutes, enactments, orders or regulations or other similar instruments of general application and any other rules, instruments or provisions in force from time to time relating to the processing of personal data and privacy applicable to the performance the cloud service. Specifically, where applicable the Data Protection

Act 1998, the Data Protection Bill, the Regulation of Investigatory Powers Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and the GDPR (Regulation (EU) 2016/679), as amended or superseded.

2.5 Operational Security

Operational Security *- The service provider should have processes and procedures in place to ensure the operational security of the service.*

PeaSoup operate strictly to an overall security policy which ensures that all critical information assets are protected against unauthorised access. Information is protected from accidental or deliberate disclosure. Integrity of information is maintained. Information assets are available for operational activities in line with SLA's defined by information owners. Business continuity plans are developed, maintained and tested. All applicable legal, regulatory and compliance obligations are met. Unauthorised use of information or information systems are prohibited in accordance with published policies. The security policy, supporting policies and standards are communicated and acknowledged by all relevant employees and third parties as deemed appropriate. All aspects of the security program are routinely audited to ensure compliance on an annual basis. All data storage adheres to the Information classification and handling policy to ensure that data is handled and stored in a secure manner, retained for an appropriate period only, and then disposed of in such a way that it should not be possible for that information to be reused.

2.6 Personnel Security

Personnel Security *- Service provider staff should be subject to personnel security screening and security education appropriate for their role.*

PeaSoup operates a security policy whereas basic checks are undertaken on employment with references and official documents to verify identity. Staff are security rated with defined degrees of access to the datacentre operations dependant on their role and access points to the datacentre, both physical and electronic are audited and secured.
Everyone working for PeaSoup has a duty of care for safeguarding the confidentiality, integrity and availability information and are required to comply with this and related Information Security Policies. All the servers both physical and virtual that comprise of the management and underlying customer infrastructure have strong passwords and require individual user account access, there is no access via root or administrator passwords for any staff and all access is audited and justified.

2.7 Secure Development

Secure Development *- Services should be designed and developed to identify and mitigate threats to their security.*

All development is undertaken in line with our Software Development Policy internal policy. This 10-page formal process defines ensures that all software has an independent environment separating development, test and production systems, where updates and patches are only permitted in dev and all changes are reviewed with full testing process. This policy also defines the use of data for testing to ensure the data is not production data or where required the data is sanitised before use. Software security testing is performed in a test environment that simulates the live environment in terms of platform, processor, load & performance. All development and changes are subject to a code review and management acceptance and must conform to the change control procedures in line with the PeaSoup Change Control Policy.

2.8 Supply Chain Security

Supply Chain Security *- The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.*

The PeaSoup supply chain consists of hardware, software and professional service suppliers. All hardware is source from reputable sources and shipped from manufacturer, all hardware specified is confirmed via a published compatibility list to ensure there is full support and compatibility, tested against all software components of the cloud. An example is that the prime hardware suppliers is Fujitsu, renowned for their existing work with government contracts, tested and compatible with all VMware, Veeam and Zerto software components that create the full cloud service.
Where professional services or support services are sourced then the PeaSoup Supplier Security policy applies to all trusted third parties, contractors and suppliers who have a business requirement to access any data owned or controlled by PeaSoup. PeaSoup ensures that all third parties are made aware of any pertinent internal policies and they are required to comply with all policies in the same manner as PeaSoup staff with the same restrictions and auditing of all access. All third parties have contractual agreements and are bound by non-disclosure agreements. Overall the use of third parties is kept to a minimum and only used for specialist skills to enhance the PeaSoup support service levels. All software is installed in house to our documented specifications.

2.9 Secure Consumer Management

Secure Consumer Management *- Consumers should be provided with the tools required to help them securely manage their service.*

Authentication of consumers to management interfaces and within support channels Customers administer their PeaSoup virtual Datacentre resources through a portal interface, which provides access to all virtual machines, networking configurations and security edge devices. Each customer as a unique URL and web access to the portal is secured by industry-standard Transport Layer Security (TLS) 1.2 connections using 2048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC. Additionally, a customer may choice to interact with the vDC management via API calls to the same URL with the same levels of protection. All the features and capabilities of eh PeaSoup cloud are available to each customer and fully configurable from the management interface. On the initial creation of virtual Datacentre by PeaSoup staff an administrative user is created for that customer and the login details sent to the relevant person as part of the service agreement and initial setup. On the creation of the vDC PeaSoup provide each new customer with a full walk though of all the portal features. The customer administrative account has a timed lockout based on failed login attempts. It is the role of this user to create any other users in the system and secure their rights through define roles, which can be linked to another authentication process via LDAP if desired to prevent duplicate password management. Using the role-based access system users can be created and limited to specific network segments in a read only or full access position. PeaSoup provide a support operation to assist in any configuration requirements and whilst there are no restrictions as to who can telephone, email or log a support call through the support portal, there are strict controls on the level of information that can be provided back to that person. Any person requesting a password reset from the PeaSoup support desk will be refused and referred to their own administrator. Any administrator looking to reset their password will only be permitted after additional call back checks are in place and the first attempt will be to reset to the original without resending the documentation.

2.10 Identity and Authentication

Identity and Authentication *- Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.*

Users are created within each virtual Datacentre (vDC) using either a locally created user or a remote authentication source with LDAP or SAML. Role based access is utilised to define the level of access, with read only access or denied access to certain elements by default. The administrator of the vDC can define granular roles for example creating specific firewall security function roles or creating development users who have restricted access to all but a specific ring-fenced development network.

2.11 External Interface Protection

External Interface Protection *- All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.*

The PeaSoup cloud consists of the management cluster where the only outbound service is the management portal interface and the backup portal interface. These web-based services are protected behind two physical firewalls, restricted in traffic below the scale of the network connectivity, in a failover pair with full inspection of all traffic across the only open ports. All web traffic is secured across SSL connections.
The backup provides authenticated access to backup the services in the vDC and restore to the vDC, there is no other functionality.
The management portal provides the main access and configuration of the vDC and is protected by an additional firewall / load balancer. There are two porta servers balanced for performance and failover and the service running is dynamically created and periodically reset every few hours to protect against any compromise of the system from attack.
Each vDC has its own gateway that PeaSoup rate limits the bandwidth to ensure a flood, DOS or DDOS attack does not flood the entire network and only maxes out the vDC edge device being attacked. Multiple gateways many be applied in a vDC for either segmentation, protection or scale, these provide NAT, packet filtering rules, VPNs both site and clients, Web Application Firewall (WAF) and also some deeper security inspections dropping to identify IP Spoofing, malformed TCP packets.
Within the vDC servers can be grouped into application groups (vApps), this way different networks can be applied, and security rules can be enforced on how different servers groups can communicate with each other, creating various levels of DMZ in the network.
The physical network beyond the vDC has no controls set to restrict its usage, unless direct interconnected, the main internet traffic is routed from the PeaSoup datacentre via diverse routes to two points of presence in two further London datacentres with four main providers at each point of presence to ensure full resilience.

2.12 Secure Service Administration

Secure Service Administration *- The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.*

Access to management systems are based on the bastion host principle, VPN's secured with username, password and certificates are used to access the network with a full audit trail of access. Bastion hosts are then used with individual username and password control to access administration systems, again with a full audit trail of usage with only privileged and certified users having access in line with the PeaSoup Security policies

2.13 Audit Information Provision to Consumers

Audit Information Provision to Consumers *- Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.*

The PeaSoup Audit and Monitoring policy covers the processes for managing auditing, logging and monitoring on all PeaSoup systems. Robust audit, logging and monitoring practices allow the forensic readiness and detective controls to protect critical systems effectively. In the event of an incident, the correct information is available to assist in investigation and remediation processes. The PeaSoup process has an audit, logging and monitoring procedure which informs and protects employees, customers and the company. The policy also aims to maintain productivity levels and introduces a professional standard of communication with customers and business partners. To ensure accuracy, all system clocks are synchronised to a reliable time source within the datacentre and the time source in the datacentre is configured to a single external time source.
From a consumer perspective there is monitoring and other audit information that can be gathered against all elements of the vDC. This information can help to understand the overall position, however most customers prefer to utilise their own pre-existing auditing tools that interrogate the servers from within the virtual machines. Installing agents or information gathering tools from directly within each virtual machine provides a more granular audit where information can be retrieved from the operating system, user authentication processes and also the applications in use.

2.14 Secure use of the Service by the Consumer

Secure use of the Service by the Consumer *- Consumers have certain responsibilities when using a cloud service for this use to remain secure, and for their data to be adequately protected.*

PeaSoup provide the virtual Datacentre and all the tools to protect the environment. The same security rules apply to that of a physical datacentre and whilst PeaSoup can assist and advise in the configuration based on our internal security policies there is always a recommendation that independent penetration testing is contracted by each customer to ensure full protection. It is the responsibility of each customer to ensure that security is implemented, appropriate to the service. It is expected that each customer will have their own information security and other policies to apply to their virtual Datacentre.