CONTENTS

PCI DSS COMPLIANCE FOR YOUR WEBSITE

This guide should be read in conjunction with our **Security Policy** which can be found on our website or obtained from our Sales team.

When processing credit/debit card information, we recommend you limit your risk exposure by outsourcing credit/debit card processing to a third-party PCI DSS Approved Payment Service Provider and processing only non-PCI compliant data at your side.

If you choose to process or store Cardholder Data or process Sensitive Authentication Data on any of our services you must meet the requirements of the PCI DSS Requirements and Security Assessment Procedures.

To assist you with PCI DSS compliance the following is a guide provided in good faith to help you evaluate your compliance with each requirement based on our understanding of Payment Card Industry (PCI) Data Security Standard, v3.1; you are responsible for ensuring that you meet each of the requirements.

BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

We offer multi-tier firewall protection as standard on our Cloud VPS and Jelastic services.

At network and physical server level we periodically filter traffic to high-risk ports (particularly if a zero-day vulnerability is identified in any software we are using), suspicious traffic patterns and similar behaviour.

Customer servers are configured with firewalls pre-configured to use a default ruleset specific to the type of service being deployed. Firewalls can be further configured to customer requirements (such as restricting access to certain services, ports or protocols) via customer control panels or upon request to our support team.

All software firewalls on managed servers may be managed by Layershift proactively (e.g. to implement additional protection during a widespread attack against our infrastructure or customers, or to allow our monitoring system access to monitor a specific service).

Your responsibility:

- ⚠ **Assess the risks and work and implement a custom firewall ruleset specific to your requirements.**

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

We do not use vendor-supplied passwords or encryption keys on any of our infrastructure or customer servers, and default accounts are removed or strengthened (e.g. using strong encryption keys instead of passwords, or restricting access to certain source IP addresses). No physical or virtual server has any wireless internet connectivity.

By default we only deploy services likely to be required on any new server and we can work with you to remove certain services upon request.

Protocols considered Insecure (e.g. SSL and early versions of TLS) are either disabled by default or can be disabled upon request; these should be identified when you run a PCI DSS vulnerability scan and can be disabled by our support team.

Your responsibilities:

- ⚠ **Determine if you need to split your servers into separate role-based functions, e.g. by having a web server separate from a database server.**
- ⚠ **Determine if you need to disable any unnecessary services.**
- ⚠ **Determine if you need to disable insecure protocols - this could reduce compatibility with clients such as old web browsers or email clients.**

Tip: You are required to run a PCI DSS Vulnerability Assessment/Scan as part of the PCI DSS Requirements which can help you identify and resolve weaknesses covered by requirement 2. Our technical support team can assist you in implementing required changes / reporting applicable false positives to your ASV.

PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

- ⚠ **You are fully responsible for reviewing and implementing any cardholder data protection requirements for any data you store, including implementing full encryption of any data including secure key storage**

Requirement 4: Encrypt transmission of cardholder data across open, public networks

We offer a wide variety of SSL Certificates (including Extended Validation Certificates) with free installation to encrypt cardholder data submitted via your website. Our SSL department can provide pricing upon request.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

This requirement specifies that antivirus software is required on systems commonly affected systems. In practice, we usually deploy antivirus only on email services on Linux servers due to the resource overhead of antivirus on Linux and (in our assessment) the currently low risk compared to Windows systems.

For any Windows servers you should discuss this the configuration of any server antivirus with our sales department.

Your responsibility:

- ⚠ **Perform an initial assessment and periodic evaluations to determine the malware risk based on your requirements.**

Requirement 6: Develop and maintain secure systems and applications

Our security policy details the steps we take to secure infrastructure and customer servers, including:

- ✔ Monitoring of software vendor mailing lists and other sources for security updates or vulnerabilities
- ✔ Security update installation within a reasonable timeframe, particularly those we deem critical or important
- ✔ Mitigation of known high-risk attack vectors

Your responsibility:

- ⚠ **Development of secure application / website code and implementation of your own security policy. You are entirely responsible for the security of any website code you deploy.**

Tip: We suggest using our Traffic Guard PCI DSS-compliant Web Application Firewall to make compliance easier and to reduce your risk of using potentially insecure code. PCI DSS requirement 6.6 requires you to perform a full code audit (e.g. static code analysis) for every code change and at least once per year to

eliminate common code vulnerabilities (e.g. SQL injection, XSS, remote file inclusion) but you can deploy and monitor a separate Web Application Firewall to block these attack threats using our Traffic Guard solution. We recommend restricting network access to your server to only allow traffic from our Traffic Guard IP addresses.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need to know

Layershift system and technical support engineers are able to login to infrastructure and customer servers to perform their duties. All new employees are screened to BS7858 standard by a third-party employee screening specialist. Non-disclosure, confidentiality and privacy agreements are in place for all employees and any trusted suppliers with access to sensitive information.

Your responsibility:

- ⚠ **You are responsible for restricting logical access to any cardholder data you store or process, including encryption and secure key storage.**

Requirement 8: Identify and authenticate access to system components

All of our employees have individual user accounts which need to be authenticated to be able to login to any systems, and login from a Layershift office or using a secure remote IPsec VPN with brute-force protection in place. Any terminated employees are removed from our user database including VDI, VPN, office and datacentre access lists promptly. Two factor authentication is required to be able to access to any computer terminal. Minimum password complexity and expiration rules are in operation.

Requirement 9: Restrict physical access to cardholder data

Our security policy details the steps we take to restrict physical access to cardholder data, including:

- ✔ Industry-standard lockable racks within a secure, private area restricted to only our BS7858 security screened employees and datacentre engineers.
- ✔ Controlled and monitored access 24x7 with at least a valid access card, biometric identification and visual verification. CCTV at all ingress/egress points and on the datacentre roof.
- ✔ Any out of hours access is scheduled in advance by a manager.
- ✔ ISO27001 accredited datacentre with on-site BS4979 (cat II) security centre.

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

All physical access to servers is monitored via CCTV and an access control system and is logged on a 24x7 basis. All servers are configured to log access (e.g. root / admin level or user level) by default. Customer servers are configured to use brute-force protection by default, which can be tuned to customer requirements.

Your responsibility:

- ⚠ **All application level access to your data. Determine if you need additional logging such as a log management and monitoring service to be implemented.**

Requirement 11: Regularly test security systems and processes

We do not offer wireless access to infrastructure or customer servers. Remote access is restricted to an IPsec VPN with 2 factor authentication. Software security updates are installed after quality testing and in compliance with our Service Level Agreement.

Your responsibility:

⚠ **Perform regular vulnerability scans to meet the PCI DSS requirements. Determine if any other regular or initial testing is required.**

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain a policy that addresses information security for all personnel.

Your responsibility:

⚠ **Implement and maintain your own security policy that meets the PCI DSS requirements.**

APPENDIX A: ADDITIONAL PCI DSS REQUIREMENTS FOR SHARED HOSTING PROVIDERS

Requirement A.1: Shared hosting providers must protect the cardholder data environment

Our shared hosting services do not meet the requirements of PCI DSS.

In all cases it is your responsibility to determine if you meet the requirements of PCI DSS and to implement a Risk Mitigation and Migration Plan if required.