Security Policy

CONTENTS

PHYSICAL SECURITY (UK)

ACCESS CONTROL AND MONITORING

Specification

- ✔ ISO27001 accredited UK facility
- ✔ Secure compound surrounded by maintained palisade fencing
- ✔ Controlled multi-stage 24x7 access; valid access card, biometric identification, remote visual verification
- ✔ On-site BS5979 (cat II) security centre
- ✔ On-site BS8418 Alarm Receiving Centre & Remote Video Response Centre
- ✔ Priority emergency services response
- ✔ Monitored security cameras 24x7 at ingress/egress points and on the datacentre roof

Server access

- ✔ Secure, private datacentre suite
- ✔ Industry-standard lockable racks and remote access monitoring / logging
- ✔ Employee access granted only if a legitimate business need exists and after BS7858 security screening
- ✔ Out of hours access scheduled and granted in advance by a manager
- ✔ Customers and third parties prohibited from physical access

Datacentre environment

- ✔ VESDA smoke detection
- ✔ FM200 / Argonite fire suppression
- ✔ 24x7 air temperature and humidity monitoring
- ✔ 24x7 critical infrastructure monitoring, including plant room

REDUNDANCY

Datacentre

- ✔ 2(N+N) UPS with dual redundant changeover panels
- ✔ Dual power feeds to racks
- ✔ Continuous voltage regulation
- ✔ Diesel generators with fuel on-site and re-supply agreement in place
- ✔ N+1 cooling to the data floor

Physical servers

- ✔ Designed to maximise use of redundant components
- ✔ Zero downtime replacement of PSU's, fans, hard disks
- ✔ Data stored on RAID arrays (using RAID 6, 10, 60 or similar)
- ✔ Multiple network ports
- ✔ Remote out-of-band access
- ✔ In-stock spare components or hot/cold spare servers
- ✔ On-site Layershift datacentre engineers for prompt remediation

Network

- ✔ Upstream public internet connectivity using redundant connections and diverse paths
- ✔ Network infrastructure utilises power redundancy via dual PSU or Automatic Transfer Switch
- ✔ Automatic failover, where possible

PHYSICAL SECURITY (CHICAGO)

ACCESS CONTROL AND MONITORING

Specification

- ✔ SSAE-16 certified facility
- ✔ Secure campus compound
- ✔ Controlled multi-stage 24x7 access; valid access card, biometric identification
- ✔ 24x7 CCTV monitoring
- ✔ Security checkpoints and security patrols

Server access

- ✔ Secure datacentre facility
- ✔ Industry-standard lockable racks
- ✔ Customers and third parties prohibited from physical access

Datacentre environment

- ✔ Proactive fire detection and suppression system
- ✔ 24x7 air temperature and humidity monitoring
- ✔ 24x7 critical infrastructure monitoring and control

REDUNDANCY

Datacentre

- ✔ 2N UPS
- ✔ N+2 cooling to the data floor
- ✔ N+1 central chilled water plant
- ✔ 2N utility power
- ✔ Dual power feeds to racks
- ✔ Continuous voltage regulation
- ✔ BMS monitoring and control

Physical servers

- ✔ Designed to maximise use of redundant components
- ✔ Zero downtime replacement of PSU's, fans, hard disks
- ✔ Data stored on RAID arrays (using RAID 6, 10, 60 or similar)
- ✔ Multiple network ports
- ✔ Remote out-of-band access
- ✔ In-stock spare components or hot/cold spare servers
- ✔ On-site datacentre engineers for prompt remediation

Network

- ✔ Upstream public internet connectivity using redundant connections and diverse paths
- ✔ Network infrastructure utilises power redundancy via dual PSU or Automatic Transfer Switch
- ✔ Automatic failover, where possible

PHYSICAL SECURITY (PHOENIX)

ACCESS CONTROL AND MONITORING

Specification

- ✔ SSAE-16 SOC 2 audited and HIPAA certified facility
- ✔ Controlled 24x7 access; multifactor including biometric identification
- ✔ High perimeter walls
- ✔ Multi-tier security zones
- ✔ 24x7 CCTV and motion detection
- ✔ 24x7 on-site security team

Server access

- ✔ Secure datacentre facility
- ✔ Industry-standard lockable racks
- ✔ Customers and third parties prohibited from physical access

Datacentre environment

- ✔ Fire detection and suppression system
- ✔ 24x7 air temperature and humidity monitoring
- ✔ 24x7 critical infrastructure monitoring

REDUNDANCY

Datacentre

- ✔ 2N UPS
- ✔ Central chilled redundant water cooling
- ✔ Dual power feeds to racks
- ✔ Continuous voltage regulation

Physical servers

- ✔ Designed to maximise use of redundant components
- ✔ Zero downtime replacement of PSU's, fans, hard disks
- ✔ Data stored on RAID arrays (using RAID 6, 10, 60 or similar)
- ✔ Multiple network ports
- ✔ Remote out-of-band access
- ✔ In-stock spare components or hot/cold spare servers
- ✔ On-site datacentre engineers for prompt remediation

Network

- ✔ Upstream public internet connectivity using redundant connections and diverse paths
- ✔ Network infrastructure utilises power redundancy via dual PSU or Automatic Transfer Switch
- ✔ Automatic failover, where possible

PHYSICAL SECURITY (SINGAPORE)

ACCESS CONTROL AND MONITORING

Specification

- ✔ ISO27001 accredited
- ✔ Tier III Uptime Institute design certified
- ✔ Compliant with Monetary Authority of Singapore (MAS) technology risk TVRA requirements
- ✔ Controlled 24x7 access; multifactor including biometric identification
- ✔ 24x7 monitored CCTV

Server access

- ✔ Secure datacentre facility
- ✔ Industry-standard lockable racks
- ✔ Ingress/egress managed by on-site 24x7 security guards
- ✔ Customers and third parties prohibited from physical access

Datacentre environment

- ✔ VESDA smoke detection
- ✔ 24x7 air temperature and humidity monitoring
- ✔ 24x7 critical infrastructure monitoring, including plant room

REDUNDANCY

Datacentre

- ✔ N+1 UPS
- ✔ N+1 or greater cooling to the data floor
- ✔ Dual power feeds to racks
- ✔ Continuous voltage regulation
- ✔ Diesel generators with fuel on-site and re-supply agreement in place

Physical servers

- ✔ Designed to maximise use of redundant components
- ✔ Zero downtime replacement of PSU's, fans, hard disks
- ✔ Data stored on RAID arrays (using RAID 6, 10, 60 or similar)
- ✔ Multiple network ports
- ✔ Remote out-of-band access
- ✔ In-stock spare components or hot/cold spare servers
- ✔ On-site datacentre engineers for prompt remediation

Network

- ✔ Upstream public internet connectivity using redundant connections and diverse paths
- ✔ Network infrastructure utilises power redundancy via dual PSU or Automatic Transfer Switch
- ✔ Automatic failover, where possible

SYSTEM SECURITY

INFRASTRUCTURE

Vendor software updates

- ✔ Routine 24x7 monitoring of vendor mailing lists and other sources for security updates / risks
- ✔ Quality Assurance (QA) testing prior to updates on critical infrastructure
- ✔ High impact or high risk issues patches promptly (with maintenance windows scheduled if service impacting)
- ✔ Normal or low severity updates are installed during regular routine maintenance.

Security first policy

- ✔ Devices configured to use the more secure option where possible (e.g. HTTPS not HTTP, use of private networks if public networks not required, use of security keys instead of passwords, enforced use of complex passwords)
- ✔ Sensitive data transferred between sites/offices transferred using IPsec VPN with high-grade encryption
- ✔ Internal systems firewalled to secure internal network
- ✔ No use of default vendor-supplied passwords
- ✔ Remote access to secure network encrypted and restricted to employees with 2-factor authentication
- ✔ Access to critical / sensitive systems restricted to employees with legitimate business need
- ✔ Centralised logging preferred, where possible
- ✔ Brute-force protection in place, where possible
- ✔ Any major changes to infrastructure are reviewed by a manager and logged in a centralised change management system

CUSTOMER DATA

Backups

- ✔ Secure, private backup network with physical separation from customer services
- ✔ Frequent recovery points, according to your SLA
- ✔ Up to two weeks retention periods as standard, according to your SLA
- ✔ Includes log files for post-incident analysis

Vendor software updates

- ✔ Routine 24x7 monitoring of vendor mailing lists and other sources for security updates / risks
- ✔ Quality Assurance (QA) testing prior to updates on customer servers
- ✔ High impact or high risk issues patches promptly (with maintenance windows scheduled if service impacting)
- ✔ Normal or low severity updates are installed during regular routine maintenance
- ✔ Non-stop kernel updates are included for all Linux services with no interruption to service; periodic full kernel updates are scheduled periodically in advance

Secure data destruction

- ✔ Customer data permanently deleted once services are terminated; includes backups after any retention period
- ✔ Hard disks securely destroyed by data destruction specialists, or wiped using secure data destruction software

Protection

- ✔ Direct superuser level access is not granted on managed customer servers
- ✔ Brute-force protection in place on customer services, where possible
- ✔ Routine security checks performed to verify customer identity before completing sensitive support requests (e.g. requests pertaining to access, modification or destruction of customer data)
- ✔ Antivirus software with automatic virus definition updates on infrastructure and customer servers, where required (excluding Linux systems in general where antivirus is not usually required)

Security first policy

- ✔ New systems configured with latest vendor supplied software versions
- ✔ Hardened software configurations
- ✔ Unnecessary services disabled by default
- ✔ Network isolation between servers prevents IP address theft or traffic sniffing
- ✔ Access to customer data restricted to employees with business need

OTHER SECURITY

EMPLOYEES

- ✔ New employees screened to BS7858 standard
- ✔ Non-disclosure, confidentiality and privacy agreements in place for all employees and relevant suppliers
- ✔ Ongoing security training and reviews in place across all departments
- ✔ Security awareness forms key part of employee development and our company culture

CUSTOMER PAYMENT METHODS

- ✔ Customer credit/debit card processing outsourced to Level 1 PCI DSS Payment Service Provider
- ✔ PayPal payment processing fully outsourced to PayPal
- ✔ Only partial payment information stored/processed by our systems (operating to relevant PCI DSS standards for outsourced payment processing), payment methods cannot be re-charged outside of Layershift merchant accounts

DATA DISCLOSURE

Subscriber information and service use metadata

- ✔ We do not disclose subscriber information or service use metadata (generally information included in our infrastructure log files or your server log files) without your consent, except if we at our sole discretion deem it necessary to do so, such as in the following cases:
  - ✔ To selected suppliers, subsidiaries, or associated companies where essential to the provision or support of our service, and where we consider their privacy and confidentiality agreements to maintain a similar standard to that which we provide
  - ✔ In the event that you are reselling or otherwise providing services to third parties to assist your end-users to identify and contact you
  - ✔ To comply with legal process, such as a court order or other legal request from a law enforcement agency
  - ✔ To protect the interests or rights of our other customers or suppliers
  - ✔ To protect our rights or enforce our legal agreement with you
  - ✔ If your use of our service is or is reasonably suspected to be in breach of our Acceptable Use Policy
  - ✔ To prevent or reduce what we consider to be risk of injury or loss of life
- ✔ Except where disclosure arises in the course of provision and support of your service, for the purpose of assisting your end-users to identify and contact you, where prohibited by law or if we consider that doing so may result in further damages, harm, or distress, we will serve you notice of at least five business days (in the United Kingdom) to the email address registered in your customer account before disclosing any subscriber information or service metadata.

Data stored on our servers

- ✔ We do not disclose data stored on your server (except log files to provide metadata as above) without your consent, except in the following cases:
  - ✔ To comply with legal process, such as a court order or other legal request from a law enforcement agency
  - ✔ To protect our rights or enforce our legal agreement with you
  - ✔ To prevent or reduce what we consider to be risk of injury or loss of life

- ✔ Except where prohibited by law or if we consider that doing so may result in further damages, harm, or distress, we will serve you notice of at least five business days (in the United Kingdom) to the email address registered in your customer account before disclosing any data.

CUSTOMER RESPONSIBILITIES

You as the customer are responsible for maintaining secure website code; running insecure code on a fully up-to-date and secure server does not make your website secure. You are solely responsible for ensuring compliance with any legal, regulatory or contractual security requirements in your use of our services.

We may provide security services including but not limited to firewalls, intrusion detection and prevention, web application firewalls, denial of service protection. Although we will always try to appropriately balance the needs of maximum security and service usability, it may not always be possible to protect your service from every attack. New attacks methods are devised every day, and therefore we cannot guarantee 100% effectiveness of any security device, configuration, or method deployed as part of our service. We are unable to accept responsibility for any losses incurred as a result of any breach of security, and you are advised to maintain appropriate cyber risks insurance as appropriate for your own business needs.

The following best practice recommendations may assist you in improving your security posture:

- ✔ Keep your passwords, phrases and security keys secure (e.g. for passwords use minimum complexity rules such as mixed character types, minimum length)
- ✔ Frequently change login credentials to reduce the risk of successful attacks or malicious access
- ✔ Ensure only users with a legitimate need have access to your login credentials or services
- ✔ Keep any application code you deploy up-to-date
- ✔ Use secure programming best practices when writing your own code (e.g. OWASP Secure Coding Practices)
- ✔ Subscribe to vendor mailing lists for any applications you use (e.g. WordPress) to ensure visibility of any announced security risks
- ✔ Consider deploying our Traffic Guard PCI DSS-compliant Web Application Firewall to reduce your risk level against zero-day vulnerabilities, e.g. SQL injection, XSS, remote file inclusion and other OWASP top 10 threats
- ✔ Encrypt sensitive data during transmission and at rest, where possible