PageGroup

Supplier Compliance Standard

CONTENTS

Purpose of this document

This Supplier Compliance Standard lists the security controls that PageGroup suppliers are required to adopt with when accessing PageGroup facilities, networks and/or information systems, handling PageGroup confidential information or having custody of PageGroup information assets.

Supplier is responsible for compliance with this standard by its personnel and subcontractors, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of these standards. Additional security requirements may be specified in supplier's agreement or individual statements of work.

1. Governance & Compliance

Supplier must have an Information Security Management Framework that is documented and commitment demonstrated by the Supplier‘s Senior Management. The Framework should align to the information security policies and provide assurance that information risks are being managed adequately.

Supplier must define and communicate roles and responsibilities for Information Security. These must be reviewed after any material change to the Supplier’s operating model or business.

Supplier must document a security compliance management process, which comprises information security controls derived from regulatory and legal drivers and contracts and includes an annual review of implemented information security processes and controls.

If requested, on an annual basis, supplier will complete an information security questionnaire and provide written responses (or documents) about its security practices, to enable PageGroup to assess compliance with the security requirements of these standards. Alternatively, supplier may produce independent assurance reporting in an internationally accepted standard such as ISO27000 certification or a SOC1/SOC2 Type 2 report.

Supplier will provide PageGroup with the contact information of the person(s) PageGroup may contact in relation to any information security and/or compliance issues.

2. Human Resource Security

Supplier must perform background checks, consistent with local laws and regulations, for all personnel. The level of verification performed should be proportional to risk correlated to roles within the organisation.

Supplier personnel are required to agree, in writing, to abide by supplier’s security requirements and organisational policies.

Supplier must have a security awareness program for all personnel that encompasses education, training and updates for security policies, procedures and requirements. Security Awareness training must be provided at time of hiring and repeated at regular intervals.

Supplier must have formal disciplinary processes in place for personnel and take appropriate action against personnel who violate supplier’s organisational policies.

Upon termination of employment, supplier must remove personnel access to information systems, networks and applications. Personnel must also return all company provided IT Assets.

Supplier must maintain a list of its subcontractors, the country/countries to which confidential information may be transferred to or accessed from and will provide the list to PageGroup for approval if requested. PageGroup reserve the right to reject the use of any subcontractor, provided there is reasonable justification.

2.1. Specific roles and responsibilities

Personnel involved in implementing and maintaining systems which are being used to deliver services to PageGroup must be:

- assigned clear responsibilities;
- aware of information security principles and associated good practice;
- technically capable to deal with error, exception and emergency conditions.

Personnel who maintain systems which are being used to deliver services to PageGroup must be supported by approved methods of:

- user registration and de-registration process;
- monitoring key security-related events (e.g., unsuccessful login attempts of authorised users)

- validating processes/data;
- reviewing error/exception reports.

The risk of individuals disrupting the running of business applications, systems and networks which are being used to deliver services to PageGroup, either in error or by malicious intent, must be reduced by:

- minimising reliance on key individuals;
- segregating the duties of individuals responsible for running business applications, systems and networks from the duties of those responsible for designing, developing and testing them;
- organising duties in a manner as to minimise the risk of fraud, theft, error and unauthorised changes.

The activities of individuals running business applications, systems and networks which are being used to deliver services to PageGroup must be monitored.

3. Data Protection

In respect of Supplier's processing or handling of personal information[1] on behalf of PageGroup, both Supplier and PageGroup will comply with all applicable requirements of the applicable data protection laws.

Supplier shall provide any assistance reasonably required by PageGroup in order to help it fulfil its obligations under applicable data protection laws.

Supplier shall maintain complete and accurate records of all information necessary to demonstrate compliance with data protection law. Such records must include records of staff training; records of processing activities and technical and organisational measures taken to ensure compliance with data protection law. Supplier shall make such records available to PageGroup or PageGroup's auditors on demand.

Supplier shall assist and provide information as PageGroup reasonably requires in order to demonstrate the Supplier's or PageGroup's compliance with data protection law including PageGroup's obligations relating to data security and conducting data protection impact assessments;

Supplier shall permit PageGroup or its external advisers (subject to reasonable and appropriate confidentiality undertakings) to inspect and audit the data processing activities carried out by the Supplier personnel and comply with all reasonable requests or directions of PageGroup to enable PageGroup to verify that the Supplier is in full compliance with its obligations under applicable laws;

Supplier shall notify PageGroup within 24 hours if the Supplier or any of its sub-processors discovers any actual or suspected data breach involving personal information. Likewise, Supplier shall notify PageGroup within 24 hours if the Supplier or any of its sub-processors receives a complaint, request or communication relating to the processing of PageGroup personal information. Supper shall provide PageGroup with full co-operation in fulfilling PageGroup's obligations under data protection laws in relation to any data breach, complaint, request or other communication made in respect of any personal information.

3.1. Supplier as Data Processor

Where Supplier is deemed by PageGroup to be a Data Processor, the requirements in this section applies.

Supplier shall process personal information only for the purposes of performing the services agreed in a contract with PageGroup and only in accordance with instructions provided by PageGroup in

[1] *Personal information is information that relates to an identifiable individual as set out in any applicable national privacy legislation or regulations. In Europe this includes the General Data Protection Regulation GDPR.*

writing from time to time. Supplier will inform PageGroup immediately if, in the Supplier's opinion, any instruction from PageGroup is in breach of, or is likely to breach, data protection law;

Supplier will not transfer any personal information to any third country outside the European Economic Area and Switzerland, unless authorised in writing by PageGroup and then subject to any conditions that may be imposed by PageGroup.

Supplier shall not engage any sub-processor (or allow any existing sub-processor to process personal information), without obtaining PageGroup's prior written consent, and then subject to any conditions that may be imposed by PageGroup.

With respect to each sub-processor, before the sub-processor first processes personal information, Supplier shall carry out adequate due diligence to ensure that the sub-processor is capable of providing the level of protection for personal information required by this standard; ensure that the arrangement between the Supplier and sub-processor is governed by a written contract including terms which offer at least the same level of protection for personal information as those set out in this standard and meet the requirements of data protection law.

Where a sub-processor fails to fulfil its obligations under data protection law, the Supplier shall remain fully liable to PageGroup for the performance of the sub-processor's obligations, and shall be fully liable for the acts or omissions of the sub-processor.

4. Asset Management

Supplier must maintain an accurate inventory of all IT assets used to provide services to PageGroup and must review it on a regular basis to ensure it remains current, complete and accurate.

4.1. Mobile Devices

Mobile devices (including laptops, tablets and smartphones) used to access PageGroup information must be built using standard, technical configurations and subject to security management practices to protect information against unauthorised disclosure, loss and theft.

Smartphones, tablets and other devices used to access PageGroup information using mobile operating systems and the applications that run on them, must be configured to protect the data stored on them in the event of loss, theft or cyber-attacks by deploying appropriate mobile device management controls.

Mobile devices used to access PageGroup information must be provided with secure means of connecting to other devices and to networks.

It is not permitted to store PageGroup information on employee-owned devices.

4.2. Portable Storage Devices

Generally speaking, the use of portable storage devices, such as USB memory sticks or external hard disk drives, to store PageGroup information is not permitted. Where this is required, its use must be subject to approval by your PageGroup representative.

When approved, portable devices which store PageGroup information must be encrypted using an appropriate cryptographic solution such as Bitlocker or Apple FileVault.

Users of portable storage devices utilised to store PageGroup information must be prohibited from sharing the device with unauthorised individuals and disclosing passwords (for accessing the device and encrypting files) to unauthorised individuals.

5. Access Management

Supplier must have in place access management processes which include as a minimum management authorisation prior to creating/amending/deleting accounts, periodic user access review and prompt removal of access when it is no longer needed.

Suppliers must have access controls implemented for information systems, networks and applications that verify the identity of all users and restrict access to authorised users. Each user must be identified by a unique user ID so that users can be linked to and made responsible for their actions.

Access to PageGroup information must be restricted, and with due consideration of the need-to-know, the least privilege and the segregation of duties principles.

Supplier will only access PageGroup information systems, networks and applications for the purposes of performing the services specified in the agreement with PageGroup. Supplier will not access any other PageGroup systems, networks and applications that do not form part of these agreed services.

5.1. Password Management

Strong password practices must be used, including minimum password length, complexity and expiry. Passwords must be distributed to users securely and separately from account information.

Passwords must be encrypted when transmitted between information systems, network devices and applications.

5.2. Wireless Access

Suppliers must have documented standards and procedures for controlling and encrypting wireless access to their Wireless networks.

5.3. Remote Access

Supplier must have documented standards and procedures covering individuals who handle PageGroup information when working in remote environments.

Remote access to the Suppliers network must be approved and restricted to authorised personnel. Remote access must be controlled by secure access control protocols, encryption and authentication.

6. Network Management

The requirements set out in this section relate to the networks under the control of Supplier which are used to access or store PageGroup information.

Supplier must have a documented network topology, inventory of network components and secure configuration standards covering all network components.

Networks must be protected by robust physical controls and be supported by accurate, up to date documentation and labelling of essential components.

Access to network devices must be restricted a limited number of authorised, technically competent personnel, using access controls which support individual accountability and be protected from unauthorised access.

Supplier must implement network security infrastructure such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and other security controls that provide continuous monitoring, have the capability to restrict unauthorised network traffic, and detect and limit the impact of attacks.

Supplier must have documented standards and procedures for managing external network access to any information systems and networks containing or accessing PageGroup information.

External access to information systems and networks must be restricted by:

- establishing 'Demilitarised Zones' (DMZs[2]) between untrusted networks;
- routing all network traffic through firewalls;
- granting access the minimum resources necessary to perform the work required;
- strong authentication including multi-factor authentication; and
- encryption of all traffic from the Internet to internal networks.

Where applicable to services provided to PageGroup, if VPN[3] access is used to connect to PageGroup networks and information systems, supplier must segregate their computers and networks that remotely connect to PageGroup (using either physical segregation or VLAN subnets) to prevent confidential PageGroup information, networks and information systems from being accessible by supplier personnel who have no need for such access.

2 *DMZ or demilitarized zone is a section of a network that exists between the intranet and a public network (such as the Internet) to protect an intranet from external access.*

3 VPN or virtual private network provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and PageGroup network

7. Secure Configuration

Supplier must have appropriate technical and management controls to protect physical and virtual servers from unauthorised access, accidental or unauthorised modification and accidental service outages. As a minimum Supplier must provide:

- restricting physical and logical access to a limited number of authorised individuals;
- system hardening and secure configuration;
- secure password settings;
- protection against malware;
- regular patching and technical vulnerability management;
- security logging and monitoring; and
- reviewing servers on a regular basis to verify that the above protections are effective.

8. Operational Security

8.1. Malware Protection

Supplier must use anti-virus and malware detection software to prevent, detect and remove malicious software. The software must provide automated signature updates. The software should have functionality to detect if anti-virus/malware software on computers has been disabled or not receiving regular updates.

Automatic virus and malware scanning checks must be carried out on all e-mail attachments that are sent to or received from external sources. Attachments that are identified as containing malicious code must be removed automatically.

8.2. Technical Vulnerability and Patch Management

A process must be established to identify and assess vulnerabilities and controls in any environment which is being used to deliver a service or product to PageGroup.

Supplier must monitor security advisories from technology vendors and other sources in relation to technical vulnerabilities of operating systems, applications and network devices, promptly evaluate exposure to reported vulnerabilities and take prompt action to address the identified exposure.

Supplier must have processes that apply patches to operating systems, applications and network devices in a standardised and prioritised manner based upon criticality and risk. If a security patch cannot be promptly applied due to requirements for testing, then effective risk mitigation controls must be implemented until such time patches can be applied.

Laptop/desktop computers should be configured to automatically receive operating system patches and updates.

8.3. Backups

Supplier must ensure that information systems, computers and software involved in the performance of the services provided to PageGroup are backed up. Backups must be tested on a regular basis to ensure they are adequate.

Confidential information that is stored on backup media must be encrypted. Where applicable, backup media that leaves supplier's facility must be protected against unauthorised access, misuse or corruption during transportation.

8.4. Logging and Monitoring

Supplier must maintain logs from information systems, network devices and applications and store log files in a secure manner.

Supplier must monitor all systems to ensure events such as hardware failure and cyber-attacks can be detected and responded to quickly and effectively.

Logs must be sufficiently detailed in order to assist in the identification of the source of an issue and enable a sequence of events to be recreated. This typically includes the date, time and source location for all access attempts and operating system and network security event information, alerts, failures and errors.

Integrity of logs files must be maintained and protected from tampering by restricting access to systems that store log files.

8.5. Information Security Incident Management

Supplier must have documented information security incident response procedures that enable the effective management of security incidents. The procedures must cover the identification, reporting, analysis, monitoring and resolution of security incidents.

Reported security incidents shall be verified and then analysed to determine their impact. All confirmed incidents should be classified, prioritised and logged.

Security incidents should be handled by a dedicated security incident response team or personnel who are trained in handling and assessing security incidents in order to ensure appropriate procedures are followed for the identification, collection, acquisition and preservation of information.

Information security incidents must be immediately communicated to the PageGroup Security Operations team at soc@page.com.

Other than as required by law, supplier may not make or permit any statements related to security incidents involving PageGroup confidential information, information systems or assets to a third-party without formal approval of PageGroup Legal Department, who can be reached at legaldepartment@michaelpage.com.

9. Cryptography

9.1. Cryptographic Solutions

PageGroup information classified as confidential, or containing personal information, must be encrypted when in transit or at rest.

The selection and implementation of a cryptographic solution must take into account the legal aspects of using encryption, including any regulatory restrictions to encryption in certain jurisdictions.

9.2. Cryptographic Key Management

Cryptographic keys used to protect PageGroup information must be managed securely, in accordance with documented standards and procedures, and protected against unauthorised access or destruction.

Suppliers must have documented standards and procedures for managing cryptographic keys used to protect PageGroup information.

Cryptographic keys used to protect PageGroup information must be protected against:

- access by unauthorised individuals or applications
- accidental or malicious destruction
- unauthorised copying

9.3. Public Key Infrastructure

Where a public key infrastructure (PKI) is used to protect PageGroup information, one or more Certification Authorities (CAs) and Registration Authorities (RAs) must be established and protected.

A PKI used to protect PageGroup information must be supported by documented standards and procedures.

The private keys of important internal CAs used to protect PageGroup information must be adequately protected to avoid unauthorised access.

10 Secure system acquisition and development

System or software development activities associated with the delivery of services to PageGroup must be conducted in accordance with a documented system development methodology.

Information security requirements must be considered when designing systems which will be used to deliver services to PageGroup. Supplier must ensure any subcontractors assisting in providing services to PageGroup provide assurance that they can meet PageGroup's security requirements.

System development activities associated with the delivery of services to PageGroup must be performed in specialised development environments, which are isolated from the live and protected against unauthorised access.

Software used to deliver services to PageGroup must be robust and reliable, and only acquired following consideration of security requirements and identification of any security deficiencies.

System build activities, including program coding and software package customisation, in relation to the delivery of services to PageGroup, must be performed by authorised individuals and inspected to identify unauthorised modifications or changes.

Systems under development, which will be used to deliver services to PageGroup, must be tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.

Systems under development which will be used to deliver services to PageGroup, must be subject to security testing (including vulnerability assessments and penetration testing).

Post-Implementation reviews (including coverage of information security) must be conducted for all new systems which will be used to deliver services to PageGroup.

Systems, which have been used to deliver services to PageGroup, that are no longer required must be evaluated, and subject to a decommissioning process, where required, taking account of relevant information, software, services, equipment and devices.

11 Supplier relationships

Supplier must have a documented process for managing the information risks associated with subcontractors who assist Supplier in delivering services to PageGroup.

The process must be incorporated into the organisation‘s procurement process and include:

- identification of critical and sensitive information;
- determining any additional security requirements;
- appetite to meet the organisation's security requirements;
- establishing a method for terminating, renewing and renegotiating contracts with external suppliers and providing alternative arrangements in the event that an external supplier is no longer capable to continuous to provide its services.

Evaluation of subcontractors must include the identification of any PageGroup information that will be shared with and accessed by the subcontractor.

Contracts with subcontractors must include obligations and security arrangements which specify:

- approval for any outsourcing or sharing of PageGroup information;
- the requirements for subcontractors to meet the same security requirements as Supplier;
- the need for continuous performance and security monitoring;
- reporting of any security incidents to PageGroup via Supplier.

12 Business Continuity and Disaster Recovery

Supplier must have implemented a Business Continuity program which includes a Disaster Recovery (DR) strategy. This program and related plans must be designed to ensure that Supplier can continue to function through operational interruption and continue to provide the services specified in its agreement with PageGroup.

Supplier must ensure that the scope of the Business Continuity program covers all locations, personnel and information systems that are used to perform services for PageGroup.

The Business Continuity (BC) and Disaster Recovery (DR) plans must be tested on a regular basis and the test results must be documented. Supplier must provide upon request documentation for PageGroup review to confirm that tests are being performed.

Supplier must promptly notify their PageGroup business contact in the event the DR or/and BC plan is executed and report the potential impact on supplier's capability to perform services to PageGroup.

13 Physical and Environmental Security

Supplier facilities must have physical security protections commensurate with the physical threats that Supplier facilities are exposed to. Access to all Supplier locations must be limited to authorised personnel and approved visitors. All visitors must be required to sign a visitor register. Entry points should have security cameras.

Supplier personnel and authorised visitors must be issued identification cards. Visitor identification cards must be distinguishable from Supplier personnel identification cards and must be retrieved and inventoried.

Access cards and keys that provide access to secure areas and information processing facilities such as data centres must be monitored and limited to authorised personnel. Regular reviews of access rights must be performed and logs detailing access must be stored.