HALKYN CONSULTING LTD

Supplier Security Assessment Questionnaire

Security Self-Assessment and Reporting

This questionnaire is provided to assist organisations in conducting supplier security assessments. It is designed to be provided to the supplier (with minimal editing to enter company & supplier names) who completes it as a self-assessment questionnaire. The nature of this document means cannot be used as a replacement for a formal, on-site, security assessment by a qualified professional but it can be used to help allocate resources and prioritise site visits.

Supplier Security Assessment Questionnaire (SSAQ)

This SSAQ has been issued by [Company Name] to [Supplier Name] to serve as a preliminary assessment of the security controls provided as part of the requested service. On completion [Company Name] will make a decision as to the level of physical audit required. Any deliberately false statements on this assessment will be treated as a breach of contract / disqualify [Supplier Name] from tendering services under this agreement [delete as applicable].

Instructions: ***Please provide a detailed response to each question. For questions that are not applicable to the services provided to [Company Name], please mark the question as "N/A" and provide an explanation.***

Part 1: Document Control

Supplier Name & Address:	
Assessment Completed by:	
Date of assessment:	
Additional Documents Provided	□ Relevant Network Diagram □ Relevant Security Diagram □ Relevant System Architecture □ Technical Interface Design □ Relevant 3rd Party Security Assessment(s) (e.g. SAS 70, Pentests, etc.)

Part 2: Policy Compliance

Control Area	Control Question	Supplier response
Security Policies	Does your organization have a documented information security policy?	
	What is the time interval at which security policies are reviewed and updated?	
	Who is responsible for security policy development, maintenance, and issuance?	
	Are all security policies and standards readily available to all users (e.g., posted on company intranet)?	

Control Area	Control Question	Supplier response
Policy Coverage	Select the security areas which are addressed within your information security policies and standards: □ Acceptable Use □ Remote Access / Wireless □ IT Security Incident Response □ Data/System Classification □ Third Party Connectivity □ Physical Security □ Network/Perimeter Security □ Other □ Data Privacy □ Access Control □ Encryption Standards □ Anti-Virus □ Email / Instant Messaging □ Personnel Security □ Clear Desk Details:	
Policy Provision	Is a complete set of your organisation's security policies available for review?	

Part 3: Detailed Security Control Assessment

Control Area	Control Question	Supplier response
Organizational Security	Have security-related job responsibilities, including oversight and accountability, been clearly defined and documented?	
	Have the security policies, standards, and procedures been reviewed and critiqued by a qualified third party?	
	Has the security perimeter infrastructure been assessed and reviewed by a qualified third party?	
	Do your third-party contracts contain language describing responsibilities regarding information protection requirements?	
	Describe the process by which third-parties are granted privileged access to [Company Name] Data.	
Asset Classification and Control	Do you maintain an inventory of all important information assets with asset owners clearly identified?	
	Describe your information classification methods and labelling practices.	
	Describe how user access is granted to different information classifications?	
	What are your procedures with regards to the handling and storage of information assets?	

Control Area	Control Question	Supplier response
Personnel Security	Do terms and conditions of employment clearly define information security requirements, including non-disclosure provisions for separated employees and contractors?	
	Describe the screening process for all users (employees, contractors, vendors, and other third-parties)?	
	Do you conduct formal information security awareness training for all users, including upper management?	
	Do you require additional training for system administrators, developers, and other users with privileged usage?	
	Is there a formal procedure dictating actions that must be taken when a user has violated any information security policies?	
	Are all users required to sign a confidentiality agreement?	
Physical and Environmental Security	Describe the physical security mechanisms that prevent unauthorized access to your office space, user workstations, and server rooms/data centres?	
	Are all critical information assets located in a physically secure area?	
	How do you protect your systems from environmental hazards such as fire, smoke, water, vibration, electrical supply interfaces, and dust?	
	What type of fire suppression systems are installed in the data centres (pre-action, mist, wet, clean agent, etc)?	
	What physical access restrictions have you put in place? Please describe your badge access system.	
	How is contractor access granted to secure locations?	
	What exterior security is provided (i.e. gates, secure vehicle access, security cameras, etc.)?	

Control Area	Control Question	Supplier response
	Is there a natural disaster risk? What means of business continuity and disaster recovery are employed to mitigate?	
	Describe your facilities system maintenance process.	
	Are the systems configured to record system faults?	
	Do you have a formal media destruction policy?	
	Do you employ automatic locking screen savers when users' workstations remain idle after a set period of time?	
	How is the removal of equipment from the premises authorized and controlled?	
	Are logs maintained that record all changes to information systems?	
Communications and Operations Management	Describe how you segregate duties to ensure a secure environment.	
	Describe how changes are deployed into the production environment.	
	Who manages/maintains your data centre? If you use a third-party contractor to maintain your systems, describe the vetting process by which that contractor was selected.	
	How do you protect your systems against newly-discovered vulnerabilities and threats?	
	How do you prevent end users from installing potentially malicious software (e.g., list of approved applications, locking down the desktop)?	
	Do you scan traffic coming into your network for viruses?	
	How do you protect the confidentiality and integrity of data between your company and [Company Name]?	

Control Area	Control Question	Supplier response
	How do you dispose of computer media when they are no longer of use?	
	Do you keep logs of media disposal activity?	
	How is system documentation (network diagrams, run books, configuration guides, etc.) secured from unauthorized access?	
	Are backup procedures documented and monitored to ensure they are properly followed?	
	Describe how you protect information media (e.g., back-up tapes) that is shipped offsite.	
	Describe the process by which software malfunctions are reported and handled.	
	Describe your hiring process and how a new employee is granted access to network resources.	
	Describe the process by which a non-employee (e.g., contractor, vendor, and customer) is granted access to network resources.	
	How many users will have privileged access to systems containing [Company Name] Data?	
	What processes and standards do you follow for incident management, problem management, change management, and configuration management?	
	Please describe the technical platform that supports the monitoring, maintenance and support processes (both hardware and software platforms).	
Access Control	Please describe your Access Control Policy.	
	Describe your account and password restrictions for internally facing applications.	
	Describe your account and password restrictions for externally facing applications.	

Control Area	Control Question	Supplier response
	Describe your authentication methods used to authenticate users and or third parties via external connections.	
	Do you conduct periodic checks on users' accesses to ensure their access matches their responsibilities?	
	Describe how you segment your network (i.e. security zones, DMZs, etc).	
	Do you enable any remote administration capabilities on your servers and network devices? If so, which protocol(s) do you use?	
	Describe any controls which are used to monitor and record system and application access.	
	Do workstations or production servers currently utilize any type of Host Intrusion Prevention or Detection software?	
	To what extent are user's system use logged and monitored?	
	Are failed login attempts recorded and reviewed on a regular basis?	
Development & Maintenance	What tools and technologies do you utilize to effectively manage the development lifecycle?	
	Do you use data sets containing personal information from actual people when testing an application? If so, what measures do you take to protect that information?	
	Are your test systems secured in the same manner as your production systems?	
	Describe how you protect your application source libraries	
	Do security specialists conduct technical reviews of application designs?	
	Are security professionals involved in the testing phase of an application?	
	Describe how you protect your applications from covert channels and Trojan code.	

Control Area	Control Question	Supplier response
	During the course of a software development project, when do you typically start to discuss the security design requirements?	
	Have your developers been trained in secure coding techniques?	
	Describe your techniques to handle input and output validation when designing a software application.	
	Do you assess the risks around messaging to determine if message authentication is required?	
Information Security Incident Management	Has a dedicated Information Security Response Team been established?	
	Has the Incident Response Team been trained in evidence gathering and handling?	
	Are incident reports issued to appropriate management?	
	After an incident, are policies and procedures reviewed to determine if modifications need to be implemented?	
Business Continuity Management	Has an organizational disaster recovery plan coordinator been named and a mission statement identifying scope and responsibilities been published?	
	Has a "worst-case" scenario to recover normal operations within a prescribed timeframe been implemented and tested?	
	Has a listing of current emergency telephone numbers for police, fire department, medical aid and company officials been strategically located throughout all facilities and at off-site locations?	

Control Area	Control Question	Supplier response
	Is the backup site remote from hazards that endanger the main data centre?	
	Have contracts for outsourced activities been amended to include service providers' responsibilities for Disaster Recovery Planning?	
	Have lead times for communication lines and equipment, specialized devices, power connectors, construction, firewalls and computer configurations have been factored into the Disaster Recovery Plan?	
	Is at least one copy of the Disaster Recovery Plan stored at the backup site and updated regularly?	
	Are automatic restart and recovery procedures are in place to restore data files in the event of a processing failure?	
	Are contingency arrangements in place for hardware, software, communications and staff?	
Compliance	Are the security policies and procedures routinely tested?	
	Are exceptions to security policies and procedures justified and documented?	
	Are audit logs or other reporting mechanisms in place on all platforms?	
	When an employee is found to be in non-compliance with the security policies, has appropriate disciplinary action been taken?	
	Are audits performed on a regular basis?	
	Are unscheduled/surprise audits performed?	
	Has someone been identified as responsible for managing audit results?	