Air Connect Engineering (Thailand) Co., Ltd

61/71-72 Thaveemitra 8 Alley, Rama 9 Rd., Huaykwang, Bangkok 10310 Thailand

Customer Profile

FOR

Cyber Security

(Prerequisite Checklist)

Questionnaire for container and Multipurpose Terminals.

Overview:

Table of Contents

Part 1 : GENERAL INFORMATIONS

No.	Question	Answer	Remarks
1	Type of Business?		BFSI/Manufacture/etc
2	How many employees are in your company? (required)		HO xxx / Brach xxx
3	How many employees are use computer?		Laptop / PC
4	How many of branch of office?		Load balance
5	How many MPLS link or Cloud system?		Redundant
6	How many ERP , CRM .,etc 3rd party application ?		Cloud / Premise
7	How many applications development by in-house IT Staff?		API Interface
8	How many system implement which provide by outsource(SI)?		Service Type

Part 2 : STANDARD CYBERSECURITY

Governing Policies

Governing Policies	Y/N	Remarks
Do you have an effective risk governance structure including executive management support?		
Do you currently have a Network Security policy?		
Do you currently have an Employee Separation policy?		
Is there a policy for laptops and all other mobile devices to protect data including encryption?		
Do you have a policy controlling mobile and removable computer media?		
Do you have or are you planning on acquiring Cyber-Insurance?		

Compliance Concerns

Compliance Concerns	**Y/N**	**Remarks**
Are specific regulatory or compliance concerns needed (e.g., SOX, ISO, HIPAA, GLBA)?		
If compliance is required, is it currently being met?		

Network Security

Network Security	**Y/N**	**Remarks**
Do you protect your networks against internal and external attacks with firewalls?		
Do you filter out unauthorized or malicious content including malware and viruses?		
Do you have a monitoring strategy that addresses reviewing alerts and logs?		
Have you changed all default (factory set) passwords on all networking equipment including routers and personal computers?		
Do you consistently remove or disable user accounts when an employee leaves the company?		
Are users required to change their passwords frequently using a strong password formula?		

Security Testing

Security Testing	Y/N	Remarks
Do you have an Incident Response or Disaster Recovery plan?		
Have you had a third-party security audit including vulnerability and security scans?		
If an independent audit was performed, was it more than 12 months ago?		

Part 3 : Cyber Security Questionnaire

POLICY

Cyber Security Questionnaire	Answer	Remarks
When was the last time your firm conducted and documented an independent information security risk assessment?		
Has your firm implemented a written information security plan that addresses all the gaps discovered from the assessment?		
Has your firm implemented a comprehensive threat management program that includes alerting based on intrusions beyond malware or viruses?		
Does your firm have a tested incident response plan with clearly assigned responsibilities?		
Do you have an information security awareness training program in place for your employees and contractors?		
Do you have tested business continuity?		
Do you have SIEM/Log manager implemented?		
Do you have data loss prevention (DLP)?		
Do you have a vendor management program?		

Additional Note

INCIDENT

Question	Y/N	Remarks
Does your organisation have a password policy in place and provide training to staff on how it works?		
Do you have different levels of User Account Control?		
Have you got a scheduled backup strategy in place?		
Do you have a frewall in place that is switched on and properly confgured?		
Have you got Anti-Virus installed and confgured within your organisation?		
Do you use Two-Factor Authentication where possible?		
Have you got mobile device management (MDM) in place with software such as Find My iPhone?		
Do you install the latest software updates on all devices and switch on automatic updates with periodic checks?		
Have you applied restrictions to prevent users downloading 3rd party apps?		
Have you set up encryption on all offce equipment using products such as Bitlocker for Windows or FileVault (on mac OS)?		
Do you train staff on how to spot the obvious signs of a phishing attempt and have a reporting process in place for such attempts?		
Do you train staff on the issues with Wi-Fi networks and how to use alternative options (eg VPN/Mobile network).		
Do you have an incident response plan in place in the event of a cyber attack?		
Have you changed all default passwords on any networking equipment?		
Have you ever had a vulnerability assessment or penetration test conducted on your network or websites?		
Do you have a Bring Your Own Device (BYOD) Policy in place for employees who use personal devices for work?		
Do you have a secure, encrypted way for employees working from home to access your corporate network?		
Do you log activity on your network and have the capability to identify suspicious behavior?		
Do you adhere to the UK Government's Cyber Essentials Standard?		