Information Security Policy for Service Express Subcontractors and Suppliers

Document Control

Operational Subject	Suppliers and Subcontractor compliance
Document Title	Information Security for Service Express Subcontractors and Suppliers
Author	Daren Schofield
Classification	Restricted

Revision History

See table at end of document

Release Distribution

Company Intranet

Procedure Governance

Level	Name / Department
Accountable	Senior Leadership Team
Responsible	All subcontractors and suppliers
Consulted	CISO, CCO, Contractual & Legal Principal, Supplier Relationship Manager

Reviewers and Approvals

Name	Position		Date
Derek Waterman	CCO	D. Waterman	23.2.2021

NOTE: Document versions numbered with a letter "1.a, 1.b", are draft status and therefore can be changed without formal change control but not issued into production. Once a document has been formally approved and issued its version number "Version 1" and subsequent releases will be consecutively numbered.

1.0 Purpose

This Policy defines the security measures that all Service Express Subcontractors and Suppliers requiring access to Blue Chip IT Systems (whether to access Service Express environments or indirectly gain access to Service Express client environments) must comply with.

2.0 Scope

This Policy applies to all Subcontractors and Suppliers that use Service Express IT Systems for accessing information, electronic or otherwise held by Service Express or Service Express clients.

3.0 Definitions

CCO – Service Express Chief Compliance Officer

CISO – Service Express Chief Information Security Officer

IT Systems – Service Express networks, systems and other information technology infrastructure, whether used for internal company business operations or to provide services to Service Express clients

Staff – Service Express employees (full time and part time, temporary and permanent), Contractors, Apprentices, Work Experience workers, Agency workers.

Subcontractor - Person or entity that provides software, professional services, support and/or managed services to Service Express clients with a need to interact with the IT Systems in order to be able to carry out their engagements and/or tasks, including accessing Service Express client environments

Supplier - a third party providing IT services or products to Service Express and/or indirectly, Customers.

Sponsoring Business Unit - Specific team/s within Service Express on whose behalf the Subcontractor Supplier is undertaking a particular task or engagement

4.0 Risk

Failure of a Subcontractor or Supplier to comply with Service Express information security requirements as described herein may compromise the integrity of Service Express and/or Service Express client confidential and proprietary information. This could include inadvertently allowing the introduction of computer viruses or malware into the IT Systems, thus rendering the IT Systems (and/or those of Service Express clients) more vulnerable to threats such as disruption attacks and unauthorised access.

5.0 Policy objectives

The objective of this Policy is to identify, enable and maintain adequate security measures for Subcontractors and Suppliers that have requested and been given access to work within Service Express secured IT Systems.

Subcontractors and Suppliers must adhere to all Service Express security policies during their engagement(s) with Service Express and ensure that their employees and any other parties engaged by them do likewise.

Any other relevant policies (including accompanying detail such as required technical controls) than those described in this document will be provided to each Subcontractor or Supplier at the time of an engagement with Service Express. All policies are subject to change at the discretion of Service Express.

6.0 Responsibilities

It is the responsibility of the Service Express Supplier Relationship Manager to ensure Subcontractors and Suppliers are provided with, understand, and agree to comply with this Policy.

It is the responsibility of the Service Express Compliance Function to review the level of effectiveness and adherence to this Policy through Subcontractor and Supplier audits or other applicable methods.

The Service Express CISO is responsible for determining the general security and other related standards that apply to all Subcontractors and Suppliers legitimately requiring access to the IT Systems, including but not limited to, the permitted methods of remote access and connectivity.

It is the responsibility of the Service Express CCO to ensure this Policy meets the needs of Service Express and the ISO27001 information security requirements.

The Sponsoring Business Unit Lead is responsible for determining the appropriate access rights to information and individual parts of the IT Systems by the Subcontractor and Supplier and for ensuring the correct process for granting such permissions of use is followed.

Subcontractors and Suppliers are responsible for ensuring criminal record checks are performed on staff accessing IT Systems and providing reasonable evidence of such checks on written request by Service Express.

It is the responsibility of Subcontractors and Suppliers who are sent this Policy, to return a signed copy within the requested time frame and maintain compliance to this Policy.

7.0 Policy

It is the Policy of Blue Chip that:

- All IT Systems are the property of Service Express and are primarily for Service Express business use. Subcontractors and Suppliers may not use them for personal purposes, or for any purpose other than in authorised Service Express business engagement(s).

- Subcontractors and Suppliers must not allow the IT Systems to be accessed by any third party unless specifically authorised by the Sponsoring Business Unit, and then only on the condition that the third party accepts in writing to abide by this Policy

- The IT Systems must not be used for any kind of distance selling, unsolicited mass communications (including email marketing) or to distribute software or any other kind of proprietary material unless authorised in writing by the Sponsoring Business Unit Lead.

- Subcontractors and Suppliers must not use the IT Systems for improper on unlawful purposes including to store, receive or send data files which are criminally obscene, and/or defamatory, or for communications which infringe any intellectual Property rights of a third party.

- Subcontractors and Suppliers may not use IT Systems to knowingly compromise other Service Express systems, networks or safeguards, or those of Service Express clients, violate the security of any website or to access third party systems not needed for authorised Service Express engagement(s).

- Subcontractors and Suppliers shall make every effort based on at least the standards stated herein to ensure all Service Express and Service Express client information is protected from inadvertent disclosure when being sent over the Internet or other open, non-Service Express networks.

- Secure File Transfer, encryption or password protection must be used when available to protect Service Express and Service Express client information in transit in accordance with Service Express Information Classification & Handling Policy which is available on request.

- Any unauthorised attempt to access information that is outside the Subcontractor's or Supplier's "need- to-know" for his/her operational purposes is prohibited and at Service Express discretion may result in all access to the IT Systems being suspended.

- Remote access to the IT Systems shall only be gained using methods approved in writing by Service Express which for connectivity over the Internet will include the use of Virtual Private Networking and encryption in line Blue Chip's current standard.

- For remote access using personal computing devices, access to IT Systems will be controlled through an access account, the granting of which will be coordinated by the Sponsoring Business Unit's Lead, and may at Service Express discretion include two factor authentication.

- Subcontractor and Supplier employees are responsible for safeguarding his or her password, user ID, security token and key, and badge, as well as protecting them from unauthorised use. The sharing and disclosure of access control information, badges, etc is strictly prohibited

- Subcontractors and Suppliers are accountable for any security or other incidents arising from improperly protected personal user IDs, security tokens or keys, and passwords. Compromised Service Express access information must be immediately changed and reported to Service Express.

- Subcontractors and Suppliers must use up-to-date industry leading malicious code protection and virus protection software for all systems and devices used to carry out Service Express business. and/or connect to the IT Systems including scanning of inbound and outbound emails.

- Subcontractors and Suppliers are prohibited from using USB sticks when laptops or other devices are connected to IT Systems, unless the USB sticks have been scanned for malware and viruses by Service Express before use and their use has been authorised in writing.

- Subcontractors and Suppliers are prohibited from attempting to bypass Service Express virus protection software or other system safeguards (e.g. when downloading or transferring information) under any circumstances.

- Subcontractors and Suppliers are not permitted to use unlicensed software when working on Service Express IT Systems and are not permitted to install any software on the IT Systems (licensed or unlicensed) without the written authorisation of the Sponsoring Business Unit.

- Personal computers, laptops and other devices containing Service Express or Service Express client information must be secured by their users from theft and unauthorised use and no device should be left unattended unless a password-engaged screensaver is used.

- Subcontractors and Suppliers must not remove equipment from Service Express facilities without management authorisation. Service Express reserves the right to audit equipment to ensure all Service Express business related information has been deleted before removal from Service Express facilities

- Subcontractors and Suppliers must report all IT Systems security incidents (e.g. malicious attacks, unauthorised access attempts, malware or virus infections, inappropriate email use, unauthorised data disclosure, etc.) immediately to the Sponsoring Business Unit

- Service Express will treat any breach of this Policy as a material default of contractual arrangements and although it will work cooperatively with Subcontractors and Suppliers to resolve the breach, Service Express reserves the right to take contractual remedies including termination.

8.0 Communication

The Service Express Supplier Relationship Manager is responsible for the awareness within Service Express of the supplier management processes as well as for communicating this Policy to all relevant Subcontractors and Suppliers.

9.0 Supplier Policy Acceptance

AGREED TO AND ACCEPTED BY:

Company: _______________________________

Signature: _______________________________

Name Printed: ____________________________

Title: ___________________________________

Date: ___________________________________

10.0 Review and Maintenance

The Compliance Team shall ensure this policy is reviewed annually to ensure it remains fit for purpose.

Revision History			
Issue Number	Issue Date	Description of Change	Authorisation
1.a	13.11.15	First draft copy	JS
1.0	12.04.16	Final copy	AR
1.0	26.06.17	Reviewed with no changes	SV
1.1	13.07.18	1. Slight amendments to section 7.0 (Policy) rules 2. Change of policy approval Director	GC
1.2	28.08.19	Change to policy approval Director	TS

1.3	24.02.20	General enhancements of the entire policy to ensure information security responsibilities for suppliers and contractors is clear.	DW
1.4	23/02/21	Annual review	DW