1. Appendix B – Coles Data Security Requirements

Definitions

The following definitions apply where they are used in these Data Security Requirements:

Agreement means the agreement between Coles and the Supplier under which the Supplier has agreed to provide certain goods, software and/or services to Coles, and which includes a requirement that the Supplier complies with these Data Security Requirements.

Authorised Party means an individual or entity that is not a party to the Agreement and that Coles has specifically authorised to have access to Coles Data at the Supplier's request.

Coles means the entity or entities contracting for the provision of the software and/or Services under the Agreement from the Supplier, irrespective of whether, for the purposes of other parts of the Agreement that party is defined in different terms.

Coles Data means information which is:

- provided to the Supplier (including its Subcontractors) for the purposes of;
- transmitted, received or stored in connection with; or
- processed, generated, compiled or modified through,

performing the Services.

Coles Security Policy means the Coles Information Security Policy which is available from Coles.

CVSS means Common Vulnerability Scoring System (CVSS), which is a free and open industry standard for assessing the severity of information technology system security vulnerabilities and can be found at the following link: https://www.first.org/cvss/.

Data Breach means unauthorised copying, use, disclosure, access, damage or destruction of the Coles Data.

Data Defect means any error, corruption, loss of Coles Data, or where Coles Data has become functionally disabled in each case as a result of anything done or omitted to be done by the Supplier in the course of providing the Services.

Data Security Requirements means the requirements and procedures set out in this document.

Good Industry Practice means the current and relevant industry standards relating to maintaining security for information technology systems including, but not limited to the standards prescribed by any of the following:

- National Institute of Standards and Technology;
- Payment Card Industry Data Security Standards;
- Open Web Application Security Project (OWASP);
- ISO27001; and
- any other standard agreed between the parties.

IT Systems means any information technology infrastructure used by a party, that stores, processes, transmits, or accesses Coles Data (and, in the case of the Supplier, includes any information technology infrastructure used by the Supplier's Personnel or Subscontractors that stores, processes, transmits, or accesses Coles Data) .

PCI Standards means the Payment Card Industry standards as set by the PCI Security Standards Council including those found at the website www.pcisecuritystandards.org.

Personnel means a party's officers, employees and agents.

Public Facing IT Systems means IT Systems that are accessible via a public IP address.

Services means the services provided by the Supplier to Coles under the Agreement, and includes any unspecified services or works which are incidental to the provision of those services.

Subcontractor refers to a company, person, licensee, franchisee or other third party provider (who is not an employee of the Supplier) who contracts with the Supplier to provide goods or perform work under the Agreement, and includes any further person contracting with that person to do so, and so on.

Supplier means the entity or entities contracted by Coles to provide the Services under the Agreement, irrespective of whether for the purposes of the other parts of the Agreement that party is defined in different terms.

Supplier's Information Security Policy means as described in section 2.2(a) of these Data Security Requirements.

1.0 DATA SECURITY REQUIREMENTS

1.1 Obligation to protect Coles Data

(a) To the extent the Supplier or its Personnel or Subcontractors:

(i) stores, processes, transmits, or accesses any Coles Data; or

(ii) accesses any Coles IT Systems,

then the Supplier must:

(iii) ensure that there is no unauthorised access to any Coles IT System;

(iv) ensure that there is no unauthorised access to, use of, copying, reproduction, transfer, release or dissemination of the Coles Data;

(v) ensure that there is no unauthorised damage to, destruction, deletion, corruption or alteration of the Coles IT System or the Coles Data, by any person or organisation;

(vi) establish an appropriate data retention policy (commensurate with the Software and Services provided to Coles under the Agreement) and securely delete Coles Data once there is no longer a reasonable need to retain the Coles Data due to any applicable law or in order for the Supplier to perform the Services; and

(vii) comply with these Data Security Requirements.

(b) Without limiting any other provision of the Agreement, ensure all Supplier Authorised Parties and Subcontractors are subject to, and comply with, the same or equivalent standards as set out in the Agreement and these Data Security Requirements, to the extent the Authorised Party or Subcontractor holds or has access to Coles Data or any Coles IT Systems.

1.2 Minimum Security Safeguards

(a) The Supplier must:

(i) maintain and enforce its own security practices, procedures and policies (**Supplier's Information Security Policy**) and:

(A) ensure the Supplier's Information Security Policy is regularly reviewed and updated to comply with these Data Security Requirements and Good Industry Practice; and

(B) ensure that all of the Supplier's Personnel are provided with training on the requirements of the Supplier's Information Security Policy as is appropriate and relevant to their role;

(ii) ensure that no errors, whether typographical, logical or otherwise, are introduced by the Supplier or its Personnel into the Coles Data, as it exists from time to time;

(iii) on written notice from Coles or on becoming aware of a Data Defect(s) in the Coles Data as a result of any act or omission of the Supplier, take such steps that are necessary to remedy the Data Defect(s) as soon as practicable at the Supplier's own expense;

(iv) subject to agreement by the parties, implement and maintain such additional security measures with regard to the Coles Data as may be reasonably requested by Coles; and

(v) when requested by Coles, complete an annual security assessment questionnaire.

(b) Where Coles Data is accessed, processed or stored on Supplier IT Systems, the Supplier must:

(i) implement and maintain a systematic method of monitoring, detecting, reporting and remediation of intrusions and incidents of the IT Systems;

(ii) ensure that Coles Data is encrypted to protect it from unauthorised use or disclosure in the following circumstances:

(A) if the Coles Data is to be transferred over public or private external networks; and

(B) while the Coles Data is in storage or at rest;

(iii) actively scan the IT Systems, incoming or new data for virus, worms, trojan horses, spyware, and other malicious code;

(iv) ensure all third party software programs that the Supplier uses to perform the Services are actively supported and maintained;

(v) not use vendor-supplied defaults for system passwords or other security parameters;

(vi) limit access to Coles Data to the Supplier's Personnel who need to access the information for the purpose of providing the Services and maintain such records and logs as are necessary to capture access and use of the Coles Data;

(vii) Implement multi-factor authentication for all remote access to the Supplier's IT Systems;

(viii) frequently implement vendor patches and workarounds to minimise vulnerabilities in Supplier IT Systems;

(ix) implement and maintain a comprehensive vulnerability management program for the Supplier's IT Systems that accesses, stores, processes, or transmits Coles Data (or otherwise accesses, or links to, the Coles IT systems) that includes a process for identifying

newly released information about security patches for the Supplier's IT Systems;

(x) implement and maintain a capability to respond promptly to security threats;

(xi) have documented change management procedures in place to govern any changes to the Supplier's IT Systems that the Supplier uses to perform the Services;

(xii) physically secure all business premises, data centres, files, servers, computers and back-up equipment, including without limitation using locks, pass cards/swipe cards and alarms;

(xiii) implement and maintain authentication and password controls for access to IT Systems including desktop access, laptop access and remote access to networks and servers;

(xiv) implement and maintain up to date and appropriate firewalls, anti-virus, data loss protection and intrusion detection software to protect all IT Systems;

(xv) perform monthly vulnerability scans on all IT Systems, and if requested by Coles, provide to Coles a summary report of the relevant findings and remediation plans;

(xvi) perform penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment) on all IT Systems and if requested by Coles, provide to Coles a summary reporting of relevant findings and remediation plans;

(xvii) implement and maintain access audit logs, and activity monitoring and recording for a period of no less than 12 months;

(xviii) unless otherwise permitted in the Agreement, keep all Coles Data within Australia and not allow anyone outside of Australia to have access to it, without the prior written approval of Coles; and

(xix) subject to section 2.2(c) below, procure Coles' consent (which Coles may withhold in its absolute discretion), before making any Coles Data available to a third party other than an Authorised Party, and then only making Coles Data available to the extent necessary to enable the Supplier to perform its obligations under the Agreement.

(c) Where the Supplier manages Public Facing IT Systems allowing access to, processing or storing of any Coles Data, the Supplier must configure the Public Facing IT Systems to:

(i) only allow the Public Facing IT System to be accessed with strong cryptographic protection of data in transit (e.g. HTTPS using TLS 1.2 or higher);

(ii) not expose other services to the internet from the same IP address (e.g. SMTP, NTP, FTP, SSH or RDP must not be exposed to the internet);

(iii) not expose software versioning in protocol headers;

(iv) prevent any administration of the Public Facing IT Systems from the Internet; and

(v) comply with Good Industry Practice in respect of security settings applicable to the service(s) being exposed.

(d) A disclosure of any Coles Data by the Supplier to any third party where it is required by law shall not be considered a breach of these Data Security Requirements or the Agreement, provided the Supplier promptly provides Coles with notice of its disclosure obligations prior to any disclosure (to the extent permitted by law) and provides reasonable assistance, at Coles request and cost, if Coles intends to contest the disclosure.

1.3 Secure Development

Where the Services require the Supplier to develop code which processes Coles Data, the Supplier must comply with in OWASP - Security by Design Principles or other Good Industry Practices in respect of secure coding standards as notified to the Supplier by Coles from time to time.

1.4 Vulnerability Management

(a) If an actual or potential security vulnerability, which may cause a Data Defect or Data Breach, is:

(i) publicly known;

(ii) identified by the Supplier, or

(iii) notified by Coles to the Supplier

the Supplier must as soon as practicable, validate the potential exposure of the Coles Data or IT Systems to the identified, actual or potential security vulnerability.

(b) Where the security vulnerability could reasonably be expected to cause a Data Defect or Data Breach:

(i) the Supplier must take reasonable steps to mitigate the risks associated with the vulnerability within timeframes reasonably commensurate with the risk associated with the vulnerability; and

(ii) if the vulnerability is rated with a CVSS Score of 8 or above, the Supplier must on request from Coles, provide a remediation plan demonstrating the steps being taken to mitigate the risk associated with the vulnerability.

1.5 PCI Standards Compliance

If the PCI Standards are applicable to the Services, without limiting any of the Supplier's obligations under the Agreement, the Supplier must:

(a) be aware of the PCI standards as found at the website https://www.pcisecuritystandards.org/;

(b) comply with the PCI Standards;

(c) maintain its certification confirming that it is compliant with the PCI standards;

(d) acknowledge in writing they are responsible for the security of cardholder data they possess or otherwise store, process, or transmit on behalf of Coles;

(e) document and acknowledge which PCI requirements they agree to manage on behalf of Coles;

(f) if the Supplier undergoes its own PCI assessment, provide evidence to Coles and/or its PCI assessor to verify the scope of their PCI assessment and the relevant requirements which were determined to be in place; and

(g) if the Supplier provides input into the Coles PCI assessment, provide evidence to Coles and/or its PCI assessor to verify that the relevant PCI requirements are in place.

1.6 Breach Notification and Incident Investigation Support

(a) In the event of an actual or suspected Data Breach impacting IT Systems or Coles Data, the Supplier must notify Coles in accordance with the applicable service levels under the Agreement, or if there is no applicable service level then in writing no later than four (4) hours after the Supplier becomes aware of the situation, by contacting the following contact person(s) using the method specified below:

Primary Coles contact: Computer Security Incident Response Team (CSIRT)
Phone: +61 (0)427 697 710

(b) The Supplier agrees to assist Coles internal incident investigations by providing upon request, relevant audit logs, or access to such logs.

(c) The Supplier must comply with all reasonable directions of Coles in respect to responding to an actual or suspected Data Breach.

1.7 Supplier Personnel

(a) If the Supplier's Personnel or Subcontractors have access to Coles Data or Coles IT Systems, the Supplier must agree to conduct background checks on all Personnel or Subcontractors that will have such access.

(b) If Supplier's Personnel or Subcontractors have access to Coles IT Systems, the Supplier must agree to:

(i) immediately notify Coles of any change in the Personnel's employment status or termination of the engagement of the Subcontractor, so that Coles can remove access to Coles IT Systems; and

(ii) instruct the Personnel and Subcontractors to abide by Coles Security Policy.

1.8 Right to Audit

In addition to or as part of any other audit rights under the Agreement, the Supplier agrees:

(a) Coles may request that an appropriate auditor or expert (selected and appointed by Coles) provide an assessment of the data protection processes implemented to comply with these Data Security Requirements. As part of any audit, Coles (or the third party auditor) may request the Supplier to audit its own Subcontractors engaged in

connection with the Agreement to assess compliance by those Subcontractors with the Data Security Requirements, and the Supplier must undertake such an audit and share its findings with Coles (or the third party auditor);

(b) such reports will be paid for by Coles and made available to Coles and the Supplier; and

(c) any items that do not comply with these Data Security Requirements and identified for remediation as a result of the audit must be fixed by and at the expense of the Supplier within a mutually agreed reasonable timeframe. Coles (or an appropriate auditor or expert selected and appointed by Coles) may audit any of the solutions or workarounds implemented by the Supplier to address the remediation items.

1.9 Right to Scan

Where Coles Data is processed or stored on Public Facing IT Systems, the Supplier acknowledges that Coles may perform automated and scheduled scans of such Public Facing IT Systems for the purposes of validating the level of protection that has been applied to the Public Facing IT Systems against security vulnerabilities.

1.10 Data Return and Deletion at Expiry or Termination of Agreement

(a) Within the lesser of 30 days or such time period as otherwise stipulated in the Agreement, after expiry or termination of the Agreement the Supplier (and its Subcontractors) shall return or destroy all Coles Data, and sanitize any retired media by employing procedures approved by Coles.

(b) The Supplier (and its Subcontractors) agrees to continue to maintain the data protection requirements outlined in these Data Security Requirements to protect any remnant Coles Data, such as offline back-up copies that cannot be feasibly returned or destroyed.

1.11 Conflict with other provisions of the Agreement

In the event of an inconsistency between these Data Security Requirements and any other provision of the Agreement, these Data Security Requirements shall take precedence to the extent of the inconsistency.