Vision Critical Data Protection Schedule

Revision: 2018.04.04

1 General

This Data Protection Schedule outlines the processes, infrastructure and policies that Vision Critical has in place to protect its systems and customer data.

2 Definitions

A. **"Backup"** means an extra copy of data to be used in the event that the original copy is damaged or unavailable. The extra copy of data is kept separately from the original copy;

B. **"Member"** means an individual invited by or on behalf of Subscriber to visit, view or comment on Subscriber Data on the Website and/or to participate in any forum, discussion, research, survey, study or any other means or form of questionnaire administered through the Solution;

C. **"Penetration Test"** means a search of software for Security Defects by a security expert without access to the system's source code;

D. **"Personal Data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

E. **"Production System"** and **"Production Network"** means a computing environment that is used to host the Solution and is subject to access controls and management processes governing the introduction of changes;

F. **"Security Breach"** means any confirmed unauthorized access to, use of, or disclosure of Subscriber Data;

G. **"Security Defect"** means a technical deficiency in the software or hardware that, if exploited, could result in unauthorized access to the Solution or the Subscriber Data;

H. **"Security Questionnaire"** means any Subscriber developed or proprietary form or any other means that collects information on the security, privacy or data protection capabilities of Vision Critical;

I. **"Security Scan"** means an automated search of a system for Security Defects without access to the system's source code;

J. "**Solution**" means the technology platform and automated services owned by Vision Critical, including all standard upgrades and updates thereto but excluding any third-party products or software that may interoperate with Vision Critical's technology platform;

K. **"Subscriber"** is a customer of Vision Critical who has entered into a subscription agreement with Vision Critical to access and use the Solution, and such term includes Subscriber's authorized users of the Solution;

L. **"Subscriber Data"** means information uploaded to or collected through the Solution by the Subscriber, or submitted directly to the Solution by Members;

M. **"Sub-Processor"** means a party that provides services to Vision Critical for purposes of delivering the Solution and may have access to Subscriber Data; and

N. **"Supplier"** means a party that provides services to Vision Critical for purposes of delivering the Solution and does not access Subscriber Data in provisioning such services.
O. **"Website"** means Subscriber's online operating instance of the Solution identified by and accessed via a domain owned by Subscriber;

3 Policies and Governance

Vision Critical has implemented the following governance structure with respect to its security and privacy policies and standards (the "**Policies**"):

A. Vision Critical's Policies have been approved by Vision Critical's executive (the "**Executive**");
B. A member of senior management is responsible for security and privacy at Vision Critical and periodically reports to the Executive and Vision Critical's board of directors (the "**Board**") on such matters;
C. Risks are centrally recorded and reported to the Executive and the Board on a quarterly basis;
D. Vision Critical periodically reviews its Policies and supporting documentation for relevance;
E. Non-compliance with a Policy requires approvals in accordance with a clear authority framework;
F. Non-compliance without authorized approval of Policies has outcomes up to and including termination of employment;
G. On a regular basis, reviews are performed within the business on compliance with a selection of the Policies. Material findings are reported to the Executive;
H. On an annual basis, Vision Critical conducts user security and privacy awareness education;
I. All employees sign-off on the Policies annually;
J. All new hires at Vision Critical receive criminal background checks where permitted by law; and
K. All employees are subject to written confidentiality agreements.

4 Data Centre Security

Vision Critical houses the Solution in enterprise class data centres that provide:

A. Independent annual audit reports of their security and availability capabilities. Such reports include but are not limited to: AICPA SSAE16 SOC1, AICPA AT100 Trust Principles SOC2 audit reports or ISO27001 certifications;
B. Redundant cooling, fire suppression, power and communications; and
C. 24x7 guard services, physical access control and video surveillance.

5 Infrastructure Security

Vision Critical has implemented the following security mechanisms:

A. The Solution is protected by firewalls or functionally equivalent technology that restricts traffic to only that which is required to provide the service;
B. Network traffic into the networking hosting the Solution is monitored by intrusion detection;
C. All access to the Solution and its supporting infrastructure is centrally logged;
D. 24/7 automated monitoring for malicious activity;
E. Bastion hosts and two factor authenticated VPN access into the Production Network; and
F. Anti-virus software.

6 Multi-tenant Environment

Vision Critical provides a multi-tenant Solution which holds data for multiple Subscribers, and provides the following protections:

A. Each Website is dedicated to a single Subscriber;
B. Websites are uniquely identified by their domain name and underlying account identifier;
C. Access to Websites are only granted to the identities directly associated with the Subscriber's account;
D. Data is logically segregated using either separate database schemas or data attributes that are used by the application code to make access decisions; and
E. Detailed infrastructure logs are not available to any Subscriber.

7 Application Security

Vision Critical provides the following controls within and around the Solution:

A. Username and password protected access to the administrator portal;
B. Authenticated access to the Website;
C. Logging of study creation/deletion/deployment as well as all user creation/modification/deletion; and
D. Secure development practices and use of safe software libraries. For the purposes of this section a "safe software library" is one that is provided by the manufacturer that is free of known security defects and is designed such that developers are forced to use the library in a manner that does not unintentionally introduce security defects into the Solution.

8 Data Encryption

A. All connections to the Solution are protected using encrypted channels including but not limited to Transport Layer Security (TLS);
B. All offsite Backups are encrypted; and
C. All systems storing Subscriber Data use disk storage that is encrypted at rest.

9 Operations

A. Vision Critical has implemented processes including vulnerability management, incident response and security patching procedures to protect against known and emerging threats.
B. Changes to Production Systems can only be implemented by authorized system administrators following a defined quality assurance, change management, and approval process.
C. Maintenance windows follow a defined schedule which shall be provided to Subscriber at least three (3) weeks in advance, with the exception of emergency maintenance, at https://www.visioncritical.com/trust/maintenance/.

10 Data Residency

A. Vision Critical's core systems, and associated data storage, are housed in a hosting facility at one of the following locations in accordance with the following:
    i. Subscribers based in the Americas are hosted in one of Amazon Web Services' availability regions in the USA;
    ii. Subscribers based in Europe, the Middle East or Africa are hosted in Amazon Web Services' availability region in Germany; and

iii. Subscribers based in Asia-Pacific region are hosted in Amazon Web Services' availability region in Singapore.

B. Vision Critical may relocate their hosting facilities and all Subscriber Data therein provided that such relocation:
   i. is posted to Vision Critical's website noted below in 10C, at least sixty (60) days in advance; and
   ii. keeps Subscriber Data within the same relative geographical region which is one of (a) North America for customers in the Americas; (b) the European Union for customers in Europe, the Middle East or Africa; or (c) Asia-Pacific for customers in Oceania, South East Asia, South Asia and East Asia

C. Vision Critical shall maintain an up-to-date list of hosting facilities at https://www.visioncritical.com/trust/legal/.

D. For clarity, Vision Critical does not comply with country-specific regulation that requires hosting of data within a specific country.

E. Vision Critical maintains a global user store to manage Subscriber administrative user account authentication and routing to the relevant hosting region as listed in 10A above. The data in this user store is housed in Canada.

11 Disaster Recovery and Business Continuity

A. Vision Critical shall maintain onsite snapshots and capacity sufficient to restore individual Websites within 48 hours with no more than 24 hours of data lost;

B. Vision Critical will maintain online duplicate copies of Subscriber's data;

C. If Vision Critical chooses to send backups of the data offsite such backups will be encrypted and the keys for the encryption will remain under Vision Critical's control; and

D. In the event of a catastrophic loss of an entire data centre, Vision Critical shall use its commercially reasonable efforts to recover Subscriber's Website.

12 Vanity Domain Names

For Subscribers that do not delegate administration of the Website's domain name to Vision Critical the following terms apply:

A. Such Subscribers are responsible for:
   i. Managing the assignment of such domain to any replacement Website setup in response to a disaster; and
   ii. Monitoring the domain name and associated Website to identify any issues with the linking of the domain name to the Website.

B. Uptime commitments as provided by Vision Critical will be limited to the Solution itself and measured against the uptime of a generic domain name managed by Vision Critical.

13 Suppliers and Sub-processors

Suppliers and Sub-processors are central to the provision of Vision Critical's Solution and services. Vision Critical shall maintain appropriate legal agreements with all Suppliers and Sub-processors to ensure compliance with the obligations laid out within this schedule and shall be responsible for its Suppliers' and Sub-processors' compliance with the terms of this Schedule. Vision Critical shall maintain an up-to-

date list of Suppliers and Sub-processors at https://www.visioncritical.com/trust/legal/ (the "**Subs Page**"). Subscribers may register to receive automated notifications of updates to the list of Suppliers and Sub-processors.

14 Delivery of Solution Services

A. The following functions for the Solution are delivered primarily from Canada but also through other Vision Critical operating countries (identified in section 15(A) below):
    i. System Administration;
    ii. Development;
    iii. Trouble shooting and defect analysis; and
    iv. Logging and monitoring.

B. Vision Critical utilizes Suppliers and Sub-processors, to deliver the Solution to the market. Such Suppliers and Sub-processors are set out in the Subs Page, and provide services including but not limited to:
    i. Data centre colocation hosting;
    ii. Cloud infrastructure and data hosting;
    iii. Cloud Backup storage and hosting;
    iv. Outbound email processing;
    v. Image hosting and processing;
    vi. Processing of aggregated, anonymized data; and
    vii. Support ticketing.

15 Delivery of Support Services

Vision Critical's corporate entities may be considered sub-processors under certain regulations and as such, these entities are included on the Subs Page for the services set out below.

A. The following Vision Critical entities are involved in providing technical support and member support to Subscriber and Members, as applicable; that is answering technical support questions raised by Subscriber and/or Members and incentive support services where ordered:
    i. Vision Critical Australia
    ii. Vision Critical Canada
    iii. Vision Critical UK
    iv. Vision Critical USA
    v. Vision Critical Germany

B. The following Vision Critical entities are involved in providing account management and other Subscriber related support services.
    i. Vision Critical Australia
    ii. Vision Critical Canada
    iii. Vision Critical France
    iv. Vision Critical Germany
    v. Vision Critical Singapore
    vi. Vision Critical South Africa
    vii. Vision Critical UK
    viii. Vision Critical USA

16 Support Access

Vision Critical may access Subscriber's Website for the purposes of providing support provided such access is logged and limited to authorized Vision Critical staff only.

17 Removed

18 Opt-in, Delivery and Unsubscribe

Vision Critical will provide the following email compliance and deliverability functionality within the Solution to assist Subscriber in complying with spam and other privacy regulation, and to ensure that emails deployed from the Solution can be authenticated by ISPs:

A. Confirmed Opt-in – Members are required to create an account and then confirm their subscription via an email delivered unique link before being added to the Website. Note that this functionality only exists for direct Member account creation, and Subscriber is responsible for obtaining the express, affirmative consent of individuals who are uploaded into the Solution by Subscriber.
B. Delivery - All email deployed from the Solution will be authenticated using Sender Policy Framework (SPF) and where available Domain Keys Identified Mail (DKIM).
C. Unsubscribe – All emails deployed from the Solution contain an unsubscribe link which remains functional for at least sixty (60) days from the date an email is deployed provided the Subscriber maintains a valid subscription to the Solution. Members may also unsubscribe via the Website.

19 Privacy Notice and Member Rights

A. Vision Critical shall not draft any legal documents, including but not limited to any privacy policy for Subscriber. Subscriber shall be solely responsible for drafting and providing its relevant privacy policies to Members within the Website.
B. Vision Critical maintains privacy policies to govern its own internal practices with regard to the secure and legal processing of Personal Data. Such policies address consent, collection limitation, data quality, limitation of use, disclosure, retention, transfers, data subject rights, and security as required by Applicable Privacy Regulation with regard to the processing of Personal Data. "Applicable Privacy Regulation" includes, but is not limited to:
    i. *The Personal Information Protection and Electronic Documents Act* (PIPEDA) of Canada;
    ii. Laws implementing Directive 95/46/EC, and after May 25, 2018 the General Data Protection Regulation 2016/679 ("GDPR");
    iii. The Federal Privacy Act 1988 of Australia; and
    iv. The Personal Data Protection Act 2012 of Singapore.

    To the extent Vision Critical processes Personal Data of EU citizens and is considered a data processor under GDPR, such processing shall be governed by the GDPR Data Protection Addendum located at https://www.visioncritical.com/trust/legal/.
C. Vision Critical will provide to Members the ability to:
    i. Directly request an unsubscribe via a Vision Critical designated email address;
    ii. Request details on Personal Data held about the Member;
    iii. Request corrections to Personal Data held about the Member;
    iv. Request deletion of Personal Data held about the Member;

v. Submit a complaint about the manner in which their Personal Data is being processed; and
vi. Exercise any other rights applicable to such Member pursuant to applicable laws and regulation including but not limited to the GDPR, subject to the terms of any agreements executed between Vision Critical and Subscriber.

Any such request will receive an initial response acknowledging receipt within two (2) business days without notice to Subscriber. Where set out in an Order or other agreement executed between Vision Critical and Subscriber, Vision Critical may process such requests without notification to Subscriber. Where handling of such requests by Vision Critical is not set out in an Order or other agreement, Vision Critical shall notify Subscriber and provide commercially reasonable support to Subscriber in Subscriber's performance of its privacy obligations;

D. Vision Critical will not disclose Subscriber Data to any third party without Subscriber's written permission. Third parties disclosed in the Master Subscription Agreement and this Data Protection Schedule, including through the mechanisms provided in Section 13, shall be deemed as having received Subscriber's prior written permission;
E. Vision Critical will not make use of Subscriber's Data for its own purposes with the exception of (i) generating metrics on Solution performance, for system monitoring or in a manner that is not identifiable of the Members or the Subscriber. For the purposes of this clause, aggregate and anonymized Subscriber Data is not considered Subscriber Data; and (ii) where permitted by the Master Subscription Agreement or an Order between Vision Critical or an affiliate of Vision Critical and Subscriber or other written consent provided by Subscriber, or where not explicitly prohibited by Subscriber in writing, make use of Subscriber Data for the for the purposes of developing and improving functionality and creating new functionality within the Solution. Where such use requires removal of Subscriber Data from the Website or Production Network, Subscriber Data will be processed in a protected environment and only accessed by an employee of Vision Critical or an affiliate of Vision Critical that is subject to inter-company data transfer agreements with all other Vision Critical affiliates; and
F. Vision Critical will retain logs containing personal information such as email addresses and IP addresses as well as actions taken on the Solution for security and monitoring purposes. Vision Critical will not use such logs or any other data to track Members across third party web sites or Vision Critical owned web sites with the exception of the Solution itself.

20 Data Deletion and Data Anonymization

A. Upon termination of the Agreement, Vision Critical will permit Subscriber thirty (30) days to export Subscriber Data from the Solution. Following such thirty day period, Vision Critical will have no responsibility to retain any Subscriber Data and will thereafter permanently delete all Subscriber Data stored within the Solution. Subscriber Data Backups shall be securely deleted or overwritten no more than ninety (90) days thereafter.
B. Upon request and if available, Vision Critical will provide Subscriber with the ability to designate specific fields within a survey as Personal Data that should be overwritten after a Subscriber specified period of time has passed. Only fields associated with Members that have unsubscribed themselves or otherwise had their account set to an inactive status will be overwritten after the Subscriber's specified period of time has elapsed. For clarity, the Member's record will be considered anonymized by the Solution when the fields specified by the Subscriber are overwritten such that they no longer contain identifying data; additionally the Solution will overwrite the Member's email address, user ID,

name and telephone number. Once overwritten the original data is retained as a Backup for a maximum of ninety (90) days thereafter.

C. Notwithstanding the preceding statements, Vision Critical does not purge security and performance log data on Subscription termination, such data is eventually overwritten from our central logging system over time. Logs generally do not contain Member-provided data although they may contain email address and IP address, and other identifying information in some cases.

21 Audit and Audit Rights

A. On an annual basis and at its own cost Vision Critical will receive an independent audit of its security and privacy capabilities by a qualified professional of Vision Critical's own choosing. Upon request Vision Critical shall provide the resulting attestation report to Subscriber;

B. Upon Subscriber's request, Vision Critical will provide a commercially reasonable timeline for addressing any material defects;

C. Vision Critical shall provide Subscriber the right to perform a security and privacy audit under the following circumstances:
    i. the attestation report referenced in 21A above is unavailable and Vision Critical cannot provide a commercially reasonable timeline for when the report will be made available;
    ii. the attestation report referenced in 21A above indicates material deficiencies in Vision Critical's controls that Vision Critical has not provided a remediation timeline for per 21B above;
    iii. Subscriber is a regulated entity and is required by law to perform its own audits of its suppliers;
    iv. Subscriber is required by a regulator or other body having supervisory authority over Subscriber to undertake an audit with the intention of validating Subscriber's compliance with relevant law or regulation; or
    v. Vision Critical has reported a Security Breach to Subscriber within the preceding three months.

D. If Subscriber is to undertake an audit as outlined in 21C, such an audit shall be performed:
    i. no more than once per subscription year unless otherwise required by a regulator or other supervisory body as described in 21C.iii and 21C.iv or in response to a Security Breach as described in 21C.v;
    ii. upon at least ten (10) business days advance written notice to Vision Critical. Such notice must include a clear scope statement and any evidence or other resources required by Subscriber;
    iii. at Subscriber's sole expense;
    iv. during Vision Critical's normal business hours; and
    v. over the course of no more than two (2) business days.

E. For clarity, any Subscriber-provided security questionnaire will be considered an invocation of audit rights which can be satisfied with an independent audit report as provided in 21A above. Vision Critical may, at its own choosing, provide one of the following in lieu of Subscriber's security questionnaire:
    i. A completed Standard Information Gathering (SIG) questionnaire provided by Shared Assessments and The Santa Fe Group;
    ii. A completed Cloud Controls Matrix (CCM) as provided by the Cloud Security Alliance (CSA) matrix; or
    iii. Another reasonably equivalent standard questionnaire.

F. Vision Critical may reasonably defer any such requests for an audit, provided Vision Critical offers an alternative date within six (6) weeks of the originally requested date, if one of following conditions occurs:
    i. Another Subscriber is currently conducting an audit; or
    ii. Vision Critical's own independent auditor is currently conducting their audit.
G. Vision Critical will provide support for Subscriber audits at its own cost, not including travel expenses, provided the required effort does not exceed two (2) business days per subscription year. Any additional effort required to support Subscriber's requirements may incur additional charges to Subscriber at Vision Critical's standard rates for such services. No additional costs will be accrued without prior agreement.

22 Security Testing

A. Vision Critical will conduct an annual Penetration Test of the Solution using an external provider determined in Vision Critical's sole discretion. Once identified Security Defects are remediated, Vision Critical will arrange for same external provider to provide confirmation thereof;
B. Vision Critical will conduct monthly Security Scans of the Solution;
C. Upon request by Subscriber, Vision Critical will provide evidence that such Penetration Testing and Security Scanning has been performed;
D. Once per subscription year and with at least ten (10) business days of notice, Subscriber or its agent, may perform its own Penetration Testing against a Website provided by Vision Critical, not the Subscriber's Website unless agreed in writing with Vision Critical. Subscriber agrees to forego this right if Vision Critical, in its sole discretion, offers an equivalently scoped report that is no more than twelve (12) months old;
E. Notwithstanding the preceding limitations of Penetration Testing frequency, additional testing to confirm that issues previously reported have been remediated are not limited in frequency;
F. Once per month, a Subscriber or its agent, may perform Security Scanning against its own Website once their methodology has been reviewed and approved by Vision Critical;
G. Such annual Penetration Testing or Security Scanning by the Subscriber does not invoke Subscriber's annual audit rights as provided in section 21 above;
H. Vision Critical may reasonably withhold approval for Penetration Testing or Security Scanning if there is reason to believe that the methodology the Subscriber or its agent will use disrupts the performance, availability or integrity of the Solution;
I. If Penetration Testing or Security Scanning by Subscriber or its agent disrupts the performance, availability or integrity of the Solution then Vision Critical may direct Subscriber to immediately stop or cause to be stopped all Penetration Testing of Security Scanning activity until such time Vision Critical is satisfied as to the reason for disruption being addressed;
J. If Subscriber elects for its agent to perform Penetration Testing and Security Scanning, then the agent must enter into a non-disclosure agreement with Vision Critical as well as agree to be liable for damages caused by its negligence or wilful misconduct. If Subscriber's agent is unable to enter into an agreement with Vision Critical, then Subscriber will agree to take responsibility for agent's actions and compliance with the terms of this Data Protection Schedule;
K. Subscriber will provide all information reasonably requested by Vision Critical on the nature of their Penetration Testing and Security Scanning activities prior to commencing their work. Such information

includes but is not limited to: source IP addresses, contact information, employee or agent names, times of testing;

L. Subscriber or its agent will comply with Vision Critical's guidance on performing Penetration Testing and Security Scanning and in return Vision Critical will furnish Subscriber with the necessary access to perform such Penetration Testing and Security Scanning;

M. If Subscriber requires that identified Security Defects be remediated, Subscriber or its agent must provide in writing the full details of the Security Defect such that Vision Critical may independently assess, replicate and verify the existence of the Security Defect; and

N. Within ten (10) business days of Vision Critical confirming the existence of the reported Security Defects Vision Critical will provide, upon request, a remediation plan in accordance with the timelines in Section 23 of this schedule.

23 Security Defect Remediation

A. Vision Critical uses industry standard scoring techniques, such as Common Weakness Scoring System (CWSS) and Common Vulnerability Scoring System (CVSS), for evaluating the severity of any identified security defect. Vision Critical utilizes version 1 of CWSS and version 3 of CVSS but may, at its own discretion, replace them with equivalent scoring techniques.

B. Vision Critical will score a security defect using the aforementioned techniques and categorize defects by impact as follows:

Common impact name	CVSS	CWSS
Critical	9.0 to 10.0	90 to 100
High	7.0 to 8.9	70 to 89
Medium	4.0 to 6.9	40 to 69
Low	0.0 to 3.9	0 to 39

C. Vision Critical will remediate Security Defects in our Solution using the following schedule once the reported Security Defect is confirmed:

Common impact name	Timing
Critical	Promptly and not more than fourteen (14) days
High	Within thirty (30) days
Medium	Within ninety (90) days
Low	Within one hundred and eighty (180) days

D. Vision Critical, at its own discretion, may implement a temporary solution to the Security Defect to achieve the timelines listed above. Such temporary solutions may include temporarily disabling or altering specific functionality, while working to implement a permanent solution to the Security Defect. Should Vision Critical choose to temporarily disable or alter functionality to address a Security Defect, Subscriber will not treat such actions as a reduction in service;

E. Vision Critical may reasonably defer remediation of a reported security defect for reasons including, but not limited to:

   a. The Security Defect is reported too late in the current release cycle to safely include relative to our change management practices;

b. A planned change or fix within will address the Security Defect in a reasonable time frame; or
c. All available resources are already working on a Security Defect of a greater impact.

F. Vision Critical may reasonably decline to remediate a Security Defect if the security defect provides no reasonable path for gaining access to Subscriber Data or the Solution.

24 Security Breaches

A. In the event of a Security Breach, Vision Critical shall:
   i. Take immediate and appropriate action to contain and mitigate the impact of the Security Breach;
   ii. Conduct an investigation into the cause of the Security Breach;
   iii. Promptly notify Subscriber of the Security Breach including any available details about the cause and impact of such Security Breach. Where required by law Vision Critical will inform the appropriate regulators after notifying the Subscriber;
   iv. Collect and preserve any information related to the cause, remediation efforts, data affected, and impact of the Security Breach;
   v. Upon request, provide Subscriber access to collected information, provided such information does not contain information of other Subscribers. Vision Critical may reasonably withhold such information that it cannot reasonably redact other Subscriber's information from;
   vi. Reasonably cooperate with Subscriber's request for assistance by providing notification to affected individuals; and
   vii. For clarity, a respondent disclosing the contents of a Website that they have been provided authorized access to, is not a Security Breach.

B. Notwithstanding the preceding, and unless otherwise restricted by law, Vision Critical may reasonably (i) decline cooperation and information sharing if the Security Breach was caused by Subscriber actions; or (ii) defer cooperation and information sharing if all available resources are occupied in dealing with the Security Breach.

C. Any of the above assistance which is provided by Vision Critical will be limited to one of the following, whichever occurs first: (a) a maximum cost of 25% of the Subscriber's annual subscription fee; (b) five (5) business days of effort; or (c) two (2) months have elapsed since the original notification of a Security Breach.

25 Subscriber Responsibilities

A. Subscriber is responsible for and will establish its own procedures to help ensure:
   i. Access to the Solution is based on user organization-defined job responsibilities.
   ii. Periodic user account review and maintenance is performed of Subscriber's administrative access to the Solution;
   iii. Periodic review of provided audit logs in the Solution, where available;
   iv. Subscriber employees receive adequate guidance on choosing strong passwords;
   v. The available security features in the Subscriber's Website are used as required when designing surveys;
   vi. Publication of a privacy policy to the Subscriber's Website;
   vii. Vision Critical's role as a data processor is clear;
   viii. Adherence to its user organization privacy policy and applicable law in establishing, maintaining and interacting with Subscriber's community;

ix. Adherence to its user organization privacy policy and applicable law in processing respondent data or when requesting Vision Critical process data;
x. Subscriber's own systems are protected from unauthorized access;
xi. Employees and agents of the Subscriber that have access to the Subscriber's Website are educated on Subscriber's security and privacy practices;
xii. In the event Subscriber and/or its authorized users encounter or are aware of a Security Breach or a privacy issue involving Vision Critical or the Solution it will be promptly reported to Vision Critical via Vision Critical's technical support;
xiii. Physical and logical access restrictions in Subscriber's offices to exported data and reports should be established, monitored, reviewed and authorized by the Subscriber's organization;
xiv. Where the subscription to the Solution is terminated, the Subscriber must inform Vision Critical in writing and promptly extract any required data from the Website before it is shut down and data deleted;
xv. Vision Critical is informed of relevant personnel changes in user organization or agents working on Subscriber's behalf;
xvi. Requests for user access are authorized internally;
xvii. The customization features, which include scripting, are used by Subscriber's employees safely in a manner that meets Subscriber's security policies; and
xviii. Members are appropriately selected and covered by any necessary confidentiality terms.

B. Subscriber shall not:
i. Use the Solution to store banking account numbers, credit card data, social insurance numbers or equivalent government identifiers;
ii. Use the Solution to send unsolicited email; or
iii. Knowingly direct Vision Critical to process or otherwise handle data in a manner that violates its obligations to Subscriber or any applicable laws.

26 Customer Success Services

Where Subscriber purchases additional support services from Vision Critical, Subscriber is solely responsible for directing any assigned Vision Critical account manager as to the proper handling of their data and for compliance with their privacy policies and applicable law. Subscriber must request that its account manager provide written confirmation as to directions provided by Subscriber. An account manager will reasonably comply with requests provided they do not incur additional costs, unreasonable efforts or violate Vision Critical policies and applicable laws.

27 Notice of Changes

From time to time Vision Critical may update its security and privacy practices:

A. Any material changes will be posted on www.visioncritical.com/trust/legal/;
B. In the event Subscriber determines any such material change(s) are not acceptable to them, Subscriber may terminate their agreement with Vision Critical as per its terms; and
C. Notification of all such material changes will be provided, at a minimum, thirty (30) days prior to the material changes coming into effect unless otherwise specified elsewhere in this schedule.