Technical and Organizational Measures (TOM)

This Technical and Organizational Measures Exhibit ("**Exhibit**") establishes the information security requirements for NICE's vendors to ensure the confidentiality, availability and integrity of NICE's Confidential Information. Vendor shall comply with the requirements under this Exhibit, and represents and warrants to the following provisions, as long as it: (i) processes Confidential Information, or; (ii) provides Vendor Solutions under the agreement/ statement of work to which this Exhibit is attached (the "**Agreement**").

In this Exhibit, "Vendor" means as defined in the Agreement and "NICE" means the NICE contracting entity in the Agreement and its affiliates. Other capitalized terms used herein but not defined in this Exhibit, have the meaning(s) ascribed to them in the Agreement.

Definitions

Applicable Privacy Law: all data privacy laws, rules and regulations that apply to the processing, use, security and destruction of Personal Data, including, as applicable, HIPAA, GDPR, GLBA, CCPA, and any other data protection and/or privacy laws and their related implementing regulations, and all legally binding regulatory guidelines, rules, operating policies, codes of practice, standard clauses and accreditations issued or approved by any relevant data protection supervisory authority, the European Commission or the European Data Protection Board.

CCPA: the California Consumer Privacy Act and its accompanying regulations.

Confidential Information: (i) has the definition in the Agreement (or, if not defined, the applicable non-disclosure agreement between Vendor and NICE), and for purposes of this Exhibit refers to NICE's Confidential Information, and (ii) includes any Personal Data disclosed to Vendor by or via NICE.

CVSS: the most current version of the Common Vulnerability Scoring System maintained by the Forum of Incident Response and Security Teams (FIRST), or a substantially similar industry-recognized vulnerability risk rating.

Data Incident: any incident or attempted incident that has, or is reasonably believed to have, resulted in any unauthorized access, acquisition, use, modification, disclosure, loss, destruction of, or damage to any Confidential Information in the possession or custody of NICE, Vendor or any third party acting on behalf of NICE or Vendor, or irregular or sustained incidents which appear to be targeting the Confidential Information or NICE transmissions.

GDPR: the EU General Data Protection Regulation (EU) 2016/679, as transposed into domestic legislation of each Member State of the European Economic Area, and in each case as amended, replaced or superseded from time to time, including any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union.

GLBA: the US Gramm-Leach-Bliley Act and its accompanying regulations, each as may be amended and replaced.

HIPAA: the US Health Insurance Portability and Accountability Act and its accompanying regulations, each as may be amended and replaced.

Personal Data: any and all information that identifies or relates to an identifiable individual under any Applicable Privacy Law, including but not limited to any "personal data" as defined by GDPR, "protected health information" as defined by HIPAA, "personal information" as defined by CCPA and "nonpublic personal information" as defined by GLBA.

Vendor Solution(s): the products and/or services provided by Vendor pursuant to the Agreement, and any Vendor product and/or services that contain Confidential Information.

Vulnerability: a weakness in the design, implementation, operation or management of any product, service, or other technology used by Vendor in connection with its performance under the Agreement, or computing environment connected, directly or indirectly, thereto, that permits, or could permit, unauthorized access, use, or modification to such product, service, technology, or computing environment.

Vulnerability Patch: a modification to a product, service, or other technology used by Vendor in connection with its performance under the Agreement, or computing environment connected, directly or indirectly, thereto, that remediates a Vulnerability.

A. General

1. Security and Confidentiality. Vendor maintains an information security program to protect information processing systems and media that contain Confidential Information, from internal and external security threats and from unauthorized disclosures that are at least equal to prevailing industry standards for such types of service locations.

2. Security Policies. Vendor must maintain information security policies that are approved by vendor's management and is published and communicated to all Vendor personnel. The policies must comply with all applicable laws, regulations or mandatory industry standards. Vendor must ensure that its contractors, service providers and other external workforce have similar policies and processes. Policies must be reviewed at least annually. Vendor must review its security policy at planned intervals or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness. Vendor must ensure that its contractors, service providers and other external workforce has a similar policy review process, and Vendor must monitor their compliance with such security policy.

3. Vendor Solutions. If Vendor provides Vendor Solutions, Vendor must maintain the development standards listed in Appendix A.

B. Access Management

4. Access Protection

4.1. Vendor must have an effective process to control and secure access to the Vendor Solutions and Confidential Information based on the principle of least privilege and on a "need to know" basis, through secure authentication, authorization mechanisms, and access control rules that reflect the heightened risk associated with the particular information system and the type of information stored therein. This process includes multiple layers of controls such as but not limited to tokens, security keys and authentication. Safeguards should be in place to prevent unauthorized individuals from obtaining access through fraud or error.

4.2. Vendor must maintain designated user accounts to ensure accountability of Vendor's personnel.

4.3. Vendor must use two-factor authentication method or equivalent controls to verify the identity of users accessing Vendor's networks and systems.

5. User Access Management. User access management to the Vendor Solutions must include effective processes for user registration and de-registration, user access provisioning, management of privileged access rights to information, information systems, utility programs, and program source code, management of secret authentication information, review of user access rights and removal or adjustment of access rights.

6. Passwords. Vendor must ensure that a password has a minimum of eight characters and contains at least two of the following parameters: (i) alphanumeric characters, (ii) uppercase and lowercase characters, and (iii) special characters.

7. Access Keys Provided by NICE. Vendor must maintain the strict confidentiality of access keys provided by NICE and must ensure that only authorized personnel use the access keys. Any changes, damages, or losses that may be incurred or suffered as a result of Vendor's failure to do so are Vendor's sole responsibility. Vendor must immediately notify NICE of any unauthorized use of Vendor's access keys or other need to deactivate an access key due to security concerns.

8. Clean Desk. Vendor must establish and enforce policies to ensure that Confidential Information is not left unattended on desktops, printers or elsewhere in an unsecured manner.

9. Data Loss Prevention. Access to non-corporate/ personal email and instant messaging solutions of Vendor must be restricted. Controls must be in place to prevent Confidential Information from being sent externally through email or instant messaging without encryption. Preventive controls must block malicious messages and attachments. Controls must be in place to prevent auto-forwarding of emails. Vendor must maintain appropriate controls to detect and prevent unauthorized removal of Confidential Information from Vendor's information systems and networks (e.g. disabling of USB ports, URL/Web filtering, training of Vendor personnel).

C. Asset Management

10. Asset and Information Management. Vendor must maintain an inventory of all Confidential Information that Vendor uses and all physical computing and software assets Vendor uses in the performance of its activities under the Agreement. With regard to encrypted information, Vendor must also maintain an inventory of encrypted Confidential Information and its transmission and the encryption method used. Vendor must also maintain an inventory of the third parties and/or locations outside of Vendor's premises that use any Confidential Information, the purpose for their use of such Confidential Information, the manner in which such Confidential Information was

provided to such third party, the transmission and encryption method (where applicable) used, and a description of the Confidential Information that was so provided.

11. Disposal of Confidential Information. Unless data retention is required for a longer period pursuant to the Agreement, Vendor must implement and maintain appropriate measures to properly dispose of Confidential Information from time to time as such information is no longer necessary for its intended purposes and upon NICE's request. Such measures must include but are not limited to: (i) destruction of Confidential Information in a manner that precludes recovery or re-creation of the information, electronically or otherwise, and (ii) effective removal from Vendor equipment and media using disk sanitizing processes appropriate for the classification of information contained therein and storage media type. At NICE's request, Vendor must provide NICE with a written log evidencing the destruction and any retention of Confidential Information and certify that it has complied with the foregoing in writing.

12. Acceptable Use. Vendor must maintain and enforce guidance on the acceptable use of information and assets which is no less restrictive than ISO/IEC 27002:2013.

D. Business Continuity

13. Business Continuity Management Policy. Vendor must have a business continuity management policy (or a comparable framework document) defining the requirements for business continuity plans and business continuity/recovery tests.

14. Business Continuity Plan. Vendor must have implemented an up-to-date business continuity plan. The plan must not be older than 12 months and has to contain as a minimum: (i) a clear description of the services provided to NICE containing all details relevant for a successful recovery of relevant processes; (ii) planning against the following scenarios: (a) loss of facility, (b) loss of IT technologies, (c) unavailability of staff, and (d) loss of Vendor provided services; (iii) recovery time objectives (RTOs) to be documented, and to be equal or lower than the NICE internal RTOs of the NICE functions supported by Vendor or RTOs committed to the applicable NICE client for which the service is provided, and; (iv) definition of roles and responsibilities to maintain the plan.

15. Business Continuity / Recovery Tests. Vendor must test its business continuity plan related to Services provided to NICE at least once every 12 months. Tests must be based on actual recovery plans and must not be simulations or table-top exercises only. Test results have to be documented.

E. Compliance

16. Security Standards and Applicable Law. During the term of the Agreement, and as long as Vendor is in the possession of, or has access to, Confidential Information, vendor must maintain (i) either an ISO 27001 certification or have a reputable independent third party conduct a review or assessment and provide a full report under the AICPA's Statement on Standards for Attestation Engagements (SSAE) No. 18, for SOC 2 Type II, and (ii) the applicable certifications and comply with the standards listed in Appendix A. Vendor agrees to promptly mitigate or correct all exceptions set forth in such attestations, reviews, and reports that may impact the Confidential Information and, upon NICE's request, provide NICE with the status of the remediation efforts. During the term of the Agreement, Vendor must maintain compliance with law applicable to itself and the services it provides.

17. Monitoring and Audit. Without limiting the Agreement, NICE, the applicable NICE client for which Vendor's service is provided, and NICE and the NICE client regulators, may monitor Vendor's compliance of its obligations under this Exhibit and conduct on-site audits by itself or by an auditor of its choice upon reasonable notice; provided that no notice is required if a regulator requests or upon reasonable suspicion of a Data Incident which will, or is likely to, compromise the confidentiality, availability or integrity of the Confidential Information, or violate any Applicable Privacy Law . Vendor must ensure that NICE has the ability to assure itself of Vendor's adherence to this Exhibit during the term of this Exhibit and for a reasonable time thereafter, and for so as long as Vendor is in the possession of, or has any access to, Confidential Information. Vendor must, upon NICE's request, provide NICE with evidence that the measures described in this Exhibit have been implemented. Vendor is obliged to secure audit and monitoring rights of its permitted subcontractors as defined in this Exhibit for NICE's benefit. Vendor must cooperate and furnish NICE with all documentation, information, assistance and access to facilities as NICE deems reasonably necessary.

F. Encryption

18. Encryption of Confidential Information. Vendor must encrypt Confidential Information to safeguard such information while in transit and in storage. At a minimum, prevailing industry-standard encryption techniques must

be employed such as the latest TLS or AES encryption. Cryptographic keys must be: (i) protected against unauthorized access, disclosure, modification, and loss, and (ii) rotated periodically.

G. Human Resources

19. Personnel Training. Vendor must train its personnel and permitted subcontractors with access to Confidential Information on, and implement, procedures to ensure the same degree of care as is used with Vendor's own confidential information, but never less than a reasonable degree of care in accordance with the security standards for the industry of the clients which Vendor serves, to prevent the unauthorized collection, use, sharing, retention/ destruction, and other inappropriate or prohibited Confidential Information handling practices. Vendor shall not, and shall require its permitted subcontractors with access to Confidential Information to not, sell, rent, or lease Confidential Information to third parties. Vendor must also conduct, at the minimum, annual security education refreshers on the use and handling of Confidential Information. Vendor must also take appropriate disciplinary measures for personnel and permitted subcontractors who fail to comply with such policies.

20. Personnel Background Checks. To the extent permitted under the applicable law, Vendor must conduct background checks in accordance with the provisions listed in **Appendix B**.

21. Information Security Officer. Vendor must appoint an officer to maintain, monitor, review and enforce Vendor's information security policies and the terms of this Exhibit.

22. Personnel Liability. Vendor must state its personnel responsibilities for information security in each agreement signed with any of Vendor's personnel and/or contractors. Vendor must communicate to each such personnel and/ or contractor the disciplinary process to take action against personnel /contractor who commit an information security breach.

H. Security Incident Management

23. Data Incidents. If Vendor becomes aware of an actual or reasonably suspected Data Incident, then Vendor must immediately: (i) take all lawful measures necessary to contain the Data Incident, and (ii) investigate the Data Incident in coordination with NICE and provide NICE with a summary regarding the Data Incident and, (iii) if Confidential Information has been compromised, full and complete details regarding the Data Incident and Vendor's remediation plan. All costs and expenses of such measures must be borne solely by Vendor.

24. Notification of Data Incidents. If Vendor becomes aware of an actual or reasonably suspected Data Incident, then Vendor must notify NICE as soon as possible (not to exceed 24 hours) if there is any evidence that an unauthorized use or disclosure of Confidential Information may have occurred. Notification of Data Incidents must be by email to Vendor's regular point of contact, as well as to the following email address: **security@nice.com**.

I. Network and Communications

25. Networks and Perimeter Security

25.1. Vendor must have at least the following measures for perimeter security: a firewall, an intrusion detection and prevention system (IDS/IDPS), and if Vendor has any public-facing services, they must reside within a demilitarized zone (DMZ).

25.2. Vendor must refrain from storing any Confidential Information on an internet-facing server or device in Vendor's DMZ. Firewalls must be used for the isolation of all environments, to include physical, virtual, network devices, production and non-production, and application/ presentation layers. Firewall management and policy must follow a process that includes restriction of administrative access and that is documented, reviewed, and approved, with management oversight, on a periodic basis. The production network must be either firewalled or physically isolated from the development and test environments. Multi-tier security architectures that segment application tiers (e.g., presentation layer, application and data) must be used.

26. Transmission of Confidential Information

26.1. Vendor must only send NICE's Confidential Information in an email message over publicly-accessible networks if one of the following conditions is met: (i) the email message is between representatives of Vendor and representatives of NICE, (ii) the content of the email has been approved in advance by NICE, and (iii) the email is encrypted using a previously approved by NICE encryption mechanism or is otherwise made secure with an approach that has been mutually agreed upon in advance by NICE and Vendor.

27. Portability of NICE Data. NICE's data and information must be available upon request, in either the original format sent by NICE or an industry standard format, so as to ensure its portability and interoperability.

28. Wireless Connection. Vendor must implement and enforce a process to detect, log and review authorized and unauthorized wireless connection access attempts (at a minimum, logs should indicate when access was initiated and terminated).

29. Remote Access

33.1. Remote access into the Vendor's networks must be approved and restricted to authorized personnel only. Remote access must be controlled by secure access control protocols, encryption and strong authentication.

33.2. If VPN is used to access NICE's networks and/ or information systems, Vendor must segregate computers that remotely connect to NICE (using either physical segregation or VLAN subnets) to prevent Confidential Information from being accessible or visible to unauthorized personnel.

J. Operations Security

30. Backup. Vendor must perform regular backups sufficient to restore services and data to NICE within the recovery times separately agreed upon, but in any case no later than 72 hours.

31. Mobile Devices. Vendor must establish and enforce a BYOD policy if Vendor allows personally-owned devices to be used in the service being provided to NICE. The policy must require adequate encryption of personally-owned devices using industry best practice with most recent versions installed.

32. Teleworking. Vendor must establish and enforce policies for remote workers and workers located outside of Vendor-owned or managed facilities. Such policies must define appropriate additional measures for protection of Confidential Information.

33. Anti-Malware and Anti-Phishing. All Vendor devices and those connected to Vendor's systems must be kept up-to-date with the latest anti-virus definitions to mitigate threats. Anti-virus tools must be configured to run periodic scans to prevent, detect, log and disposition malware and viruses. Vendor must implement best practices and security technologies to mitigate the threat of phishing.

34. Logging and Monitoring. Vendor must ensure that information security log entries are time and date stamped. Vendor must have information security logs: (i) available for review and protected to prevent changes; (ii) maintained for whichever is the greater of 12 months, a period defined by legal or regulatory requirements and mutually agreed business requirements; and (iii) monitored on a regular basis by a group independent from the operating team. The logs must include, among others, log-on failover attempts and log off attempts. Vendor must: (i) define security events; (ii) have alerting mechanism(s) in place; and (iii) forward security events to a separate and secure log host in real-time. Vendor must not disable logging of privileged system functions (e.g. administrator actions). Vendor must ensure that an alert is raised when unauthorized changes to system software or system configuration are detected, for investigation by a group independent from the operating team. Vendor must ensure that time synchronization is in place for all IT assets where the technology supports it.

35. Vulnerability Management. Vendor must run Vulnerability scans on Vendor's computing environments (which include but are not limited to the Vendor Solution if operating within Vendor's environments and Vendor's internal and external network) at least monthly and after any change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades).

36. Vulnerability Scoring. Vendor must reasonably assign a "Base" score and associated severity rating to Vulnerabilities in accordance with CVSS immediately after each Vulnerability becomes known to Vendor for Vulnerabilities in Vendor's computing environments (which include but are not limited to the Vendor Solution and Vendor's network).

37. Vulnerability Patches. Once a Vulnerability is assigned a CVSS severity rating, Vendor must install, or make available if the Vendor Solution has been delivered to NICE, Vulnerability Patches no later than the number of days from the date such Vulnerability becomes known to Vendor as follows: (i) Low: 180 days; (ii) Medium: 90 days; (iii) High: 30 days; and (iv) Critical: 5 days. If Vendor is unable to substantiate that the Vendor computing environments are free of Vulnerabilities through the above assessment, Vendor must collaborate with further testing. Vendor must also permit NICE to conduct its own Vulnerability scan. Vendor must maintain an alert status regarding the security of its computing environments, including all Vulnerabilities, Vulnerability Patches and corrective actions, by

subscribing to an industry-recognized service such as CERT (Computer Emergency Response Team). Vendor must test Vulnerability Patches prior to installation to ensure there is no disruption or degradation to the performance of the Vendor Solution.

38. Vulnerability Notification. Upon NICE's request, Vendor must provide to NICE a detailed report of all Vulnerabilities with and the Vulnerability Patches installed or made available by Vendor, or the timeline to provide Vulnerability Patches, to remediate such Vulnerabilities. Vendor must immediately inform NICE of any Vulnerabilities assigned CVSS severity rating of "Critical" and/or "High".

39. Storage of Confidential Information. Vendor must segregate and protect Confidential Information from Vendor's other client data. Storage of Confidential Information at locations that are not a Vendor-managed facility must be pre-approved by NICE.

40. Penetration Testing. Vendor must have a reputable independent third-party perform penetration tests at least once a year for all Vendor's systems and computer networks. Vendor must correct, within a period mutually agreed upon, all material issues discovered in the course of such penetration tests and provide NICE a written report that must include the tests results and the correction of all identified Vulnerabilities and risks.

41. Change Management. Vendor must maintain change management processes that include documentation of the purpose, security impact analysis, testing plan and results, and appropriate management authorization for all changes on systems processing Confidential Information.

K. Physical Security

42. Physical Security. Vendor must use safety, and physical and computer system security, procedures that are: (i) at least equal to prevailing industry standards for such types of service locations; (ii) designed to ensure the security and confidentiality of Confidential Information, (iii) designed to protect against anticipated threats or hazards to the security or integrity of Confidential Information, including but not limited to unauthorized intrusion, disclosure, misuse, alteration, destruction or other compromise of such information, and (iv) as rigorous as those procedures in effect by Vendor as of the effective date of the Agreement. Such procedures must include, among others, identification and signatures of all access requirements, escorted access of authorized personnel, intrusion detection systems and access controls.

43. Monitoring of Facilities. Vendor must employ monitoring for all areas where Confidential Information is used in a manner commensurate with the sensitivity of Confidential Information. Vendor's security controls must include, among others, closed circuit television cameras (CCTV), to ensure the above. Vendor must regularly review reports of user entry into Vendor's facilities housing Confidential Information.

L. Vendor Management

44. Engaging New Subcontractors. Vendor shall not subcontract performance of any Vendor Solutions unless NICE provides prior written consent. If NICE consents to the use of subcontractors, Vendor must obligate the subcontractors to comply with the obligations in this Exhibit and Vendor remains liable for the subcontractors' performance or lack of performance.

45. Compliance of Subcontractors. Vendor must perform due diligence and confirm that any permitted subcontractors are able to comply with this Exhibit prior to commencement and in regular intervals thereafter, and document Vendor's findings in detail sufficient to support such confirmation. Upon NICE's request, Vendor must provide NICE with a copy of the relevant contractual arrangement between Vendor and the subcontractor.

NICE may amend this Exhibit from time to time, by providing Vendor with a notice, as may be required by law or to meet evolving prevailing industry practices. If Vendor is not willing or is unable to meet the updated requirements of such amendments, NICE may terminate the Agreement upon 30 days written notice and the prorated amount of any prepaid fees shall be refunded for the period after the effective termination date.

ACCEPTED AND AGREED TO:

VENDOR

Signature _____

Print Name: _____

Date: _____

Appendix A
Development Standards

1. Secure Coding Standards

- If Vendor develops any Vendor Solutions, Vendor must implement secure coding standards, train all relevant application development personnel in secure application coding, and ensure that the Vendor Solutions are not vulnerable to known risks and exploits.
- Vendor must perform secure code reviews using automated scanning tools for the Vendor Solutions.
- If Vendor is developing Vendor Solutions specifically for NICE, Vendor must follow NICE secure software development instructions throughout the lifecycle of the software application, and Vendor must provide NICE with all relevant secure coding-related documentation.

2. Penetration Tests. Vendor must have a reputable independent third-party perform penetration tests at least once a year for all Vendor Solutions that use or have access to Confidential Information. Vendor must correct, within a period mutually agreed (or earlier if required by the Vulnerability Patches section above) upon, all material issues discovered in the course of such penetration tests and provide NICE a written report that must include the tests results and the correction of all identified vulnerabilities and risks.

3. Vulnerability Management

- Vendor must have the following controls in place, and agrees to provide to NICE applicable documentation and/or artifacts including but not limited to a full report from an acceptable vendor (e.g. Veracode) which substantiate, that the following security controls are in place for duration of the Agreement for Vendor Solutions: (i) static and dynamic code analysis during development (secure code review of the entire code base); and (ii) open source scanning and Vulnerability detection using Black Duck or a generally-recognized alternative providing similar or better third party library scanning and detection.
- Vendor must use the Open Web Application Security Project testing guide and top 10 Vulnerabilities as a mandatory reference to the application testing.
- Prior to implementation of the application, Vendor must correct, within a period mutually agreed upon, all material issues discovered in the course of such tests and provide NICE a written report of the results of the tests and the correction of all identified Vulnerabilities and risks.
- Any application deliverable that Vendor develops specifically for NICE under the Agreement will be deemed accepted only after NICE certified in writing that the deliverable meets the terms of this Exhibit and that Vendor resolved all identified Vulnerabilities and risks.
- Vendor must perform the Vulnerability scoring and patch process defined in the Vulnerability Scoring and Vulnerability Patches and Vulnerability Notification sections above for Vulnerabilities discovered during development of the Vendor Solutions.

4. Privacy By Design and Default. If the Vendor Solution is used to process Personal Data, in addition to its other obligations, Vendor must assist NICE to comply with Article 25 of the the EU General Data Protection Regulation 2016/679 ("GDPR") by implementing appropriate technical and organizational measures in the Vendor Solutions, which are designed to implement data-protection principles and protect the rights of data subjects pursuant to the GDPR, such as to permit the proper response to data subject requests, limit access on a need-to-know basis and to achieve the goal of data minimization. Vendor must integrate such safeguards into the processing by default.

Additional Certifications and Standards

- **SOC 1 Type II (applies to Vendor Solutions that may impact NICE's financial reports).** At least once a year, have a reputable independent third party conduct a review or assessment and provide a full report under the AICPA's Statement on Standards for Attestation Engagements (SSAE) No. 18, for SOC 1 Type II. Vendor agrees to promptly mitigate or correct all exceptions set forth in such attestations, reviews, and reports that may impact the Confidential Information and, upon NICE's request, provide NICE with the status of the remediation efforts.
- **PCI DSS (applies to Vendor Solutions that process cardholder data).** Maintain PCI DSS certification with regard to any system or network that handle, store or otherwise process credit card or credit cardholder data.
- **HITRUST (applies to Vendors performing services for NICE Nexidia).** At least once a year, have a reputable independent third party conduct a review or assessment and provide a full attestation, review or report for HITRUST. Vendor agrees to promptly mitigate or correct all exceptions set forth in such attestations, reviews, and reports that may impact the Confidential Information and, upon NICE's request, provide NICE with the status of the remediation efforts.

- **FedRAMP (applies to Vendors performing services for NICE CXOne (f/k/a InContact) subcontractors).** At least once a year, have a reputable independent third party conduct a review or assessment and provide a full attestation, review or report evidencing compliance with FedRAMP requirements. Vendor agrees to promptly mitigate or correct all exceptions set forth in such attestations, reviews, and reports that may impact the Confidential Information and, upon NICE's request, provide NICE with the status of the remediation efforts.

Appendix B – Background Checks

Vendor must conduct, at its expense, background checks and 5 Panel drug tests on those of its employees who will have access (whether physical, remote or otherwise and whether on or off NICE's or clients' premises) to the facilities, equipment, systems or data of NICE or its clients. Such background checks must comply with the procedures and requirements set forth below; provided that such requirements may be limited solely to the extent required to comply with the law of the jurisdiction relevant to the applicable Vendor's personnel. Vendor must keep copies of background screening documentation and provide certification of their completion to NICE when requested. NICE acknowledges that all such documentation is confidential. Vendor shall not knowingly permit an individual to have access to the facilities, equipment, systems or data of NICE or its clients if such individual (a) has been convicted of a crime or has agreed to or entered into a pretrial diversion or similar program in connection with (i) a dishonest act or a breach of trust, or (ii) a felony; or (b) uses illegal drugs. Vendor warrants to NICE that satisfactory background checks and drug tests have been done in accordance with these requirements prior to such employee being granted such access and that no personnel that have failed such checks and tests will be used for projects pursuant to this Exhibit. Vendor must also comply with any security policies, procedures or requirements of any NICE client for whom Vendor's employees will be providing the Vendor Solutions, including but not limited to further background checks or drug tests if required by such clients.

The table below lists the documents which are currently considered acceptable evidence for a specific check in the United States. Acceptable documents for other jurisdictions will be provided upon request. One piece of documentation is required per check, unless the individual has more than one activity in the specified period, in which case one piece of documentation per activity is required. Where a choice of documentation is indicated for any category, individuals should be asked to provide documentation containing their photograph wherever possible. If acceptable documentation cannot be provided as evidence by the candidate then the facts should be independently verified. For every document taken as evidence for a background check the original document must be sighted and checked for any evidence of tampering. The receiver of the documents should certify photocopies are a true copy of the original prior to shredding the document.

Check	Details	Type of acceptable documents
Proof of right to work	Check of photographic ID proving the individuals legal right to work	Confirmed via Form I-9, Employment Eligibility Verification, List A or B and C (US Federal regulations)
Proof of identity	Post-employment check of photographic ID issued by the Government to confirm identity	Candidate provides acceptable documents from List A or B and C, Form I-9, Employment Eligibility Verification. After the I-9 Form is complete an additional identify verification is conducted through the E-Verify system, which is maintained by The Department of Homeland security and in partnership with the Social Security Administration.
Proof of residency	Proof of current abode	Address information (derived from Social Security number) provides means for ensuring appropriate criminal checks are conducted.
Proof of activity	Documents establishing activities to cover: • 2 years (including current) for non-Executive employees • 5 years (including current) for Executive employees	• W2 • Pay Stub • Tax Returns • Letter from former employer on company letterhead • Verbal confirmation from former employer if contact is independently verified by Recruiter Self-Employment: Tax Returns (including business, partnership, corporate, federal, state or local)
Criminal Background Check	As permitted by applicable law, proof that individual has not pled guilty or no contest, or has not been convicted of or entered a pretrial diversion program in connection with the prosecution of any criminal offense regardless of whether described as a felony or as a misdemeanor	• A criminal background search of all court records in each venue of the person's current and previous addresses over the past seven years. Minimum of three counties. • Specific court of custody for criminal record regardless of primary index or lower court location. County courthouse searches developed off of the SSN trace address history using Felony & Misdemeanor (FAM) and Felony Including Misdemeanor (FIM) searches at the county seat plus one lower court when applicable.

	involving dishonesty, a breach of trust, or money laundering	• In the event that the person maintains or has maintained residences outside of the United States, NICE and Vendor shall agree upon the appropriate background checks.
Education Check	Proof of educational achievement	• Certificate of highest relevant degree at educational institute indicated • Verification of applicable professional certifications.