BRIGHT HORIZONS
BASELINE THIRD PARTY SECURITY REQUIREMENTS

Version 1.4 (updated September 2022)

Contents

SECTION 1:

REQUIREMENTS INTRODUCTION AND BACKGROUND

1. SUMMARY

1.1. These Baseline Third Party Security Requirements shall be applied by all external entities that store or process Bright Horizons Information on behalf of Bright Horizons and its affiliates or are critical IT service providers.

1.2. These Requirements aim to ensure that a vendor, supplier or contractor of Bright Horizons maintains the confidentiality, integrity and security of Bright Horizons information in accordance with the requirements imposed by Data Protection Laws and applicable industry standards and best practices.

1.3. These Requirements aim to provide for a minimum level of information security. However, information security threats come from a wide range of sources and are continually developing; therefore security measures shall be reviewed regularly.

1.4. Where necessary, having regard to the state of the art, industry best practice and cost of their implementation, measures that compensate for or are additional to those detailed in these requirements may be needed. Such compensating measures shall be captured on the Annexure A form (attached to these Requirements). In any event such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the information to be protected.

2. DEFINITIONS

2.1. Within these Requirements the following terms have the following meanings:

2.1.1. **"Affiliate"** means in relation to a party, any company which (directly or indirectly) controls, is controlled by and/or under common control with that party.

2.1.2. **"Data Protection Laws**" means all Laws applicable to the Processing of Personal Information (including but not limited to Data Privacy or Data Security Laws) used or obtained by the Supplier in the performance of the Services including, without limitation to, those national, state, regional and/or local laws and regulations governing privacy, security, confidentiality and protection of Personal Information.

2.1.3. "**Information Systems**" means all systems, including, but not limited to, electronic, equipment, and storage media, used by the Contractor to access, store or otherwise Process Bright Horizons Information.

2.1.4. "**Intellectual Property**" means and include patents, trademarks, service marks, trade dress, logos, trade names, domain names and corporate names, copyrights, trade secrets, know-how, and all other intangible, industrial and intellectual property rights, by whatever name known, and all registrations thereof and applications to register the same.

2.1.5. "**Financial Personal Information**" means Personal Information consisting of financial information including but not limited to bank account numbers, credit card numbers and debit card numbers (whether with or without expiry dates and pin numbers), income and credit histories.

2.1.6. "**Government Identifier Personal Information**" means Personal Information consisting of national insurance numbers, social security numbers, tax identifications, passport

numbers, drivers license numbers or other equivalent government issued identifiers.

2.1.7. **"Personal Information"** has the meaning given by the relevant Laws and shall include, without limitation, any data or information (regardless of the medium in which it is contained and whether alone or in combination) which may be supplied to or Processed by or on behalf of Supplier in connection with the provision of the Services, that relates to an identified or identifiable person ("**Data Subject**") including, without limitation, name, postal address, email address, telephone number and information about the Data Subject's health, opinions or beliefs.

2.1.8. "**Bright Horizons**" means the Bright Horizons entity, including Affiliate entities, that decides the purposes for which the Bright Horizons Information is Processed.

2.1.9. "**Bright Horizons Information**" means any information disclosed by or on behalf of Bright Horizons to the Contractor, including Intellectual Property, Business Information (such Bright Horizons Confidential or Bright Horizons Internal Use), Personal Information, Sensitive Personal Information, Financial Personal Information and Government Identifier Personal Information.

2.1.10. "**Processing**" means any operation or set of operations which is performed upon Bright Horizons Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, access, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, and "Process" and "Processed" shall have the appropriate corresponding meanings.

2.1.11. "**Contractor**" means the entity Processing the Bright Horizons Information on behalf of Bright Horizons and may include a Bright Horizons entity where it Processes Bright Horizons Information under the instructions of another Bright Horizons entity.

2.1.12. "**Security Incident**" means the unauthorized and/or unlawful access, acquisition, use, disclosure, modification, processing, destruction or loss of Bright Horizons Information or Information Systems Processing Bright Horizons Information whether in electronic or hard copy form, or interference with system operations in an information system, that compromises or which reasonably is anticipated would compromise the privacy, security, confidentiality, integrity or availability of Bright Horizons Information, including but not limited to (i) incidents resulting from or arising out of Contractor's internal use, Processing, or Transfer of Bright Horizons
Information, whether between or among Supplier's subsidiaries and affiliates, subcontractors or any other person or entity acting on behalf of Contractor; (ii) any other similar incident as may be so defined by relevant data protection laws that apply to Bright Horizons; provided that trivial attempts to penetrate Contractor's networks or systems that occur on a daily basis, such as scans, "pings" or other unsuccessful attempts to penetrate computer networks or systems maintained by Contractor, will not be considered a Security Incident.

2.1.13. "**Sensitive Personal Information**" means Personal Information pertaining to the racial or ethnic origin, physical or mental health condition, religious or similar beliefs or political or ideological opinions of an identified or identifiable individual.

2.1.14. **"Trusted Connection"** means Bright Horizons, in its absolute discretion, has determined that unrestricted access to the Bright Horizons network through a Bright Horizons firewall for a specific Contractor facility or location (hereinafter referred to as Secured Contractor facility) is required.

3. INFORMATION CLASSIFICATION AND SECURITY LEVELS

3.1. These Requirements are categorized into those that are Basic Level Requirements and Enhanced Level Requirements.

3.2. Basic Level Requirements shall be applied to all Bright Horizons Information.

3.3. Enhanced Level Requirements shall be applied in addition to the Basic Level Requirements for Personal Information, Sensitive Personal Information, Financial Personal Information, and Government Identifier Personal Information, and where otherwise specifically indicated in these Requirements.

3.4. Where Bright Horizons has agreed to specific additional security measures with a relevant Contractor in addition to those set out herein, generally or in relation to a specific service or platform, those measures providing the highest level of protection to Bright Horizons Information shall be applied by the Contractor.

SECTION 2

MINIMUM SECURITY REQUIREMENTS

1. MANAGEMENT OF INFORMATION SECURITY

Basic Level Requirements

1.1. The Contractor shall ensure that senior management of the Contractor accepts ultimate responsibility for ensuring that information security is properly managed and that these Requirements are implemented and adhered to by the Contractor and its staff.

1.2. The Contractor shall put into place a management structure to oversee the effective implementation and continuing development of security procedures. At a minimum this shall consist of an individual from senior management with the necessary authority to implement these Requirements and other necessary security procedures ("Information Security Officer" (or other Contractor staff duly authorized in the security document(s))).

1.3. The Information Security Officer's responsibilities shall include:

1.3.1. reviewing implementation and adherence to these Requirements; and

1.3.2. acting as a point of contact in relation to information security issues raised by Bright Horizons.

2. DOCUMENTED SECURITY POLICY

Basic Level Requirements

2.1. The Contractor shall document its security policy and procedures which address all the activities relating to the handling and management of data. Security policies and procedures shall be reviewed and/or updated at reasonable intervals and/or whenever there are material changes to the Information Systems, including those Processing Bright Horizons Information.

2.2. The security documents shall clearly identify those technical and organizational measures and practices to be implemented and followed by the Contractor to adequately protect the security of information Processed by the Contractor.

2.3. The security documents and/or guidance stipulating the procedures to be followed and measures to be implemented to satisfy the requirements contained therein, shall be published and communicated as relevant to the Contractor's employees and relevant external parties directly or indirectly involved in the Processing of Bright Horizons Information.

2.4. The Contractor shall, on request, provide Bright Horizons with access to copies of the security documents and any future updated versions of such documents.

3. HUMAN RESOURCE SECURITY

Basic Level Requirements

3.1. Contractor will conduct and complete appropriate background and/or verification checks of its employees, contractors and/or third parties to ensure their suitability for handling Bright Horizons Information prior to their Processing of any such Bright Horizons Information. This shall include at a minimum:

- Criminal history search;
- USA: SSN and address verification;
- Outside the USA, equivalent government identifier verification (if any) and address verification
- Employment verification;

3.2. Responsibilities and instructions in relation to protecting the confidentiality, integrity and security of Bright Horizons Information shall be defined and communicated in writing to employees/contractors/third parties.

3.3. Employment contracts, contracts with contractors and contracts with third party users shall contain terms setting out obligations and responsibilities in relation and appropriate to maintaining the confidentiality, integrity and security of Bright Horizons Information.

3.4. A formal disciplinary process shall be in place for employees who violate Contractor policy and procedures relating to the Processing of Bright Horizons Information.

3.5. Upon termination of employment/engagement, an employee/contractor/third party shall return all Bright Horizons Information in his/her possession on whatever medium it is stored, and access rights to Information Systems Processing Bright Horizons Information shall be terminated.

4. TRAINING AND AWARENESS

Basic Level Requirements

4.1. Regular information security awareness, education and training suitable to an individual's role and responsibility shall be undertaken. This shall begin with a formal induction to security procedures and policies and continue throughout employment.

4.2. Access to Bright Horizons PII will require adequate security awareness training including but not limited to Social Engineering and Phishing.

4.3. Where Bright Horizons network account and/or Bright Horizons email access is granted, Bright Horizons' applicable policies and procedures including, but not limited to, those regarding Privacy and Acceptable Use (including email usage) shall be followed by Contractor personnel. Applicable policies, procedures, and training will be provided as part of the provisioning process.

5. INVENTORY OF INFORMATION

Basic Level Requirements

5.1. Media, servers, and equipment containing Bright Horizons Information shall be labelled in a way that protects the confidentiality of Bright Horizons Information and does not expressly expose the actual content.

5.2. An inventory shall be maintained in a way that provides traceability to those media,

servers, and equipment containing Bright Horizons Information.

5.3. When Bright Horizons Information and/or media containing it are being transferred between parties, a system for recording incoming and outgoing media containing Bright Horizons Information shall be set up which permits direct or indirect identification of the kind of media, the date and time, the sender, the number of media, the kind of Bright Horizons Information contained, how they are sent and the authorized person responsible for receiving them.

6. PORTABLE MEDIA/DEVICES

Basic Level Requirements

6.1. The Contractor shall only use portable devices where there is a genuine business need and where the Bright Horizons Information on the device is appropriately erased or destroyed when the defined business need has expired.

6.2. Bright Horizons Information stored on portable devices (including laptops and PDAs, external hard drives, flash drives, CDs, DVDs, tapes and other mass storage devices) shall be adequately protected from unauthorized access, loss and destruction using industry recognized mechanisms, such as encryption, inactivity timeout, or power on passwords.

6.3. Policies and procedures for using portable devices shall be maintained by the Contractor and training on these procedures shall be provided to all Contractor staff.

Enhanced Level Requirements

6.4. Any portable device containing Bright Horizons Information shall be encrypted.

7. TESTS WITH REAL BRIGHT HORIZONS INFORMATION

Basic Level Requirements

7.1. Testing prior to the implementation or modification of a relevant Information System shall not use real or 'live' Bright Horizons Information unless there is no reasonable alternative and such use has been approved by Bright Horizons in writing. Where real or 'live' Bright Horizons Information is used, it shall be limited to the extent necessary for the purposes of testing and provide evidence that the level of security corresponding to the type of Bright Horizons Information processed is implemented. For example, if Personal Information is used, the Test systems must have the same level of security used on Production Systems that process than information.

8. ELECTRONIC STORAGE AND TRANSFER OF BRIGHT HORIZONS INFORMATION

Basic Level Requirements

8.1. Controls shall be in place to ensure that Bright Horizons Information transmitted by the Contractor across any unsecured network is transferred between authorized Information Systems and resources only, and is only exchanged through industry recognized secure transfer mechanisms such as encryption.

8.2. Procedures and policies shall be in place to prevent the unauthorized transfer of Bright Horizons Information by email and web-based applications.(DLP)

8.3. All remote access and access via non-trusted networks (e.g. ISPs, cable, application service providers, DSL connections, etc.) to Information Systems Processing Bright Horizons Information, shall use at least two-factor authentication methods (e.g. Remote Access Server (RAS), SecureID, etc.) and only take place where there is a justifiable business need.

8.4. Wireless LAN products (e.g. NIC cards and access point devices) shall not be attached to networks permitting access to Information Systems Processing Bright Horizons Information or to a device connected to Information Systems Processing Bright Horizons Information without appropriate approvals from the Information Security Officer, or other Contractor staff duly authorized in the security document(s). All wireless LAN products shall:

8.4.1. use secure identification, authentication, and encryption mechanisms; and

8.4.2. where feasible, have "peer" networking connectivity settings disabled.

8.5. When Bright Horizons Confidential Information is being accessed, or transmitted, over the Internet or via a public switched network, the communications session shall utilize a secure transport mechanism such as VPN, Secure FTP, Secure Copy, Secure Shell, HTTPS using TLS with a minimum 128-bit key strength.

8.6. Bright Horizons Confidential Information shall not be stored on desktops, laptops, handheld devices, or other removable storage devices, such as diskettes, compact discs (CDs), memory sticks or similar devices.

8.7. All laptops and hand-held devices used by any Third Party to access Bright Horizons Confidential Information shall utilize full disk encryption with a minimum 128-bit key length. It is recommended that Desktops accessing Bright Horizons Confidential Information use full disk encryption.

9. BACK-UP AND RECOVERY

Basic Level Requirements

9.1. Processes and procedures shall be in place to ensure copies of Bright Horizons Information are retained to facilitate retrieval or reconstruction following loss or destruction of primary production information. Such processes and procedures shall be conducted on a regular basis and at least weekly.

9.2. The correct functioning of the back-up system must be tested periodically to confirm that it performs an accurate and complete reconstruction of the Information Systems Processing Bright Horizons Information.

9.3. Backed-up Bright Horizons Information or Information Systems Processing Bright Horizons Information held off the Contractor's premises shall be appropriately protected from unauthorized access following documented policy and procedures.

9.4. Back-up copies shall be kept at a different secure location from the site of the equipment housing Information Systems Processing Bright Horizons Information.

Enhanced Level Requirements

9.5. Backed-up Bright Horizons Information or Information Systems Processing Bright Horizons Information held on tapes, disks or other media off Bright Horizons' or the Contractor's premises shall be encrypted.

10. DISPOSAL OF INFORMATION

Basic Level Requirements

10.1. When Contractor equipment, physical documents and files, and physical media are

disposed of or reused, recognized industry or government standard measures shall be taken to prevent subsequent retrieval of Bright Horizons Information originally stored in them.

10.2. The procedures for ensuring the secure destruction/erasure of Bright Horizons Information held on Contractor equipment, in physical documents and files, and in physical media shall be formally documented and implemented.

10.3. The Contractor shall identify the roles of the persons disposing of Bright Horizons Information, including third party services, and shall provide evidence of destruction.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

Basic Level Requirements

11.1. Equipment and/or media used for Processing Bright Horizons Information shall be protected from physical and environmental threats to prevent interruption to the Contractor's activities and loss of Bright Horizons Information. For example this can be achieved by considering the following: physically securing power and telecommunications cabling; ensuring equipment is properly maintained and protected from power failures.

11.2. Equipment and/or media containing Bright Horizons Information shall be placed in secure areas to prevent unauthorized physical access, damage, and interference to the information. Measures corresponding with the nature of Bright Horizons Information being Processed shall be taken to limit physical access to that information. For example this may include access control, CCTV, and intrusion detection systems; implementing visitor entry control procedures; securing offices, rooms, and facilities; protecting against external and environmental threats; and controlling all access points including delivery and loading areas.

11.3. Equipment and media (including printed materials) containing Bright Horizons Information shall only be removed from Bright Horizons' or the Contractor's premises following prescribed a procedure/plan that prevents unauthorized access to or retrieval of Bright Horizons Information.

11.4. Where hardcopy records containing Bright Horizons Information are to be retained in manual filing systems, they shall be stored and filed according to appropriate criteria which enable the Contractor to locate the relevant records where necessary to facilitate the access, amendment or destruction of the relevant records and facilitate the exercise of the data subject rights at the request of Bright Horizons or the individual to who those records relate The making of copies of such documents must be under the control of persons authorized in accordance with the relevant security document(s).

Enhanced Level Requirements

11.5. Containers with locks or equivalent devices to prevent tampering and/or unauthorized access shall be used to store or transport hardcopy records.

11.6. Tracking of back-up and/or mass storage media containing Bright Horizons Information during transport (for example by Radio Frequency Identification (RFID) or GPS) and/or bonded courier services shall be used.

11.7.

12. PHYSICAL AND LOGICAL ACCESS

Basic Level Requirements

12.1. Contractor shall not make Bright Horizons Information publicly available without Bright Horizons' prior written consent.

12.2. Contractor shall not make any Bright Horizons Information available via a publicly available, restricted access website (i.e. URL available from outside of the Bright Horizons network), without providing evidence of successful completion of a security vulnerability test and subsequent acceptance by Bright Horizons' Security Group (Vulnerability and Threat Management).

12.3. Further technical measures shall be put in place to prevent unauthorized electronic access to Bright Horizons Information. Expectations are that these measures include, but are not limited to, firewalls, logical separation and/or intrusion prevention and detection systems.

12.4. Authorization to access Information Systems Processing Bright Horizons Information shall be granted on a need to know or do basis, authorized users shall only have access to that Bright Horizons Information necessary for them to perform their duties.

12.5. Contractor shall restrict access to Information Systems Processing Bright Horizons Information through use of adequate and appropriate identification, authentication and authorization mechanisms.

12.6. Formal procedures to control the authorization of access rights to Information Systems and services shall be developed. The procedures shall cover:

- 12.6.1. user registration and revocation;
- 12.6.2. privilege management;
- 12.6.3. user password management; and
- 12.6.4. review of user access rights.

12.7. As part of the user registration procedures, the Contractor shall:

- 12.7.1. Ensure every authorized user is issued an unique user identification (userid) prior to accessing Bright Horizons Information or Information Systems Processing Bright Horizons Information.
- 12.7.2. Maintain a list of all individuals authorized to access Information Systems Processing Bright Horizons Information that includes the unique user identification and the level of information to which the individual has access.
- 12.7.3. The Contractor shall retain a historical list of user identification assignments for the life of the underlying Information System.
- 12.7.4. User identifications shall not be reused or reissued to different people.

12.8. At a minimum of annual intervals, the Contractor shall review those individuals that it has authorized to access Information Systems Processing Bright Horizons Information and verify whether the individual still requires access and the present access level. The review shall cover personnel changing jobs.

12.9. Only authorized Contractor personnel shall be permitted to grant, alter or cancel authorized access to Bright Horizons Information., and all such access right changes shall be documented.

12.10. Authorized users shall only be allowed to access Information Systems Processing Bright Horizons Information after completing authentication procedures. Authentication procedures for access to electronic Bright Horizons Information shall be based on a password, or other authentication method (such as biometrics, passphrases, PINs, etc.) associated with the user identification code but only known to the authorized user.

12.11. Passwords shall meet prevailing legal and/or industry standards for strength and complexity, and confidentiality.

12.11.1. Password strength and complexity shall include a length not less than 8 characters and numbers, with password composition requiring three of the following four types: uppercase letters, lowercase letters, numbers and special characters. User passwords shall be configured to expire in 90 days or less.

12.11.2. Password must be changed by the user upon first access to the Information System and shall be changed at regular intervals appropriate to the information accessible via the systems to which they relate, and in accordance with Contractor security documents, prevailing industry standards and with any legal requirements applicable to the Contractor in the country in which the Bright Horizons Information is Processed.

12.11.3. Passwords shall be maintained in a location and/or format that do not compromise the security of the data they protect. Passwords will be rendered unreadable or unusable by unauthorized individuals, i.e., encrypted, when stored and transmitted electronically.

12.11.4. Access of a user identification code shall be blocked after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system. Prior to reactivation of access or replacement of lost/forgotten authentication credentials, user identity must be verified.

13. ACCESS RECORDS

Basic Level Requirements

13.1. An audit trail of access, or access logs, to Information System Processing Bright Horizons Information shall be maintained for a minimum period of one (1) year. At minimum, the audit trail shall be able to reasonably determine the files/databases accessed, user ID of the individual accessing the files/databases, the date, time and type (e.g. remote, local etc.) of access, and whether access was authorized or denied.

13.2. Access record mechanisms for producing the audit trail shall be under the direct control of the Information Security Officer, or other Contractor staff duly authorized in the security document(s), and under no circumstances can they be de-activated or manipulated.

13.3. The Information Security Officer, or other Contractor staff duly authorized in the security document(s), shall ensure that procedures are in place to detect suspicious and irregular access and requests for access to Information Systems ("Irregular Access"). Irregular Access shall be reviewed periodically and any action arising from that review shall be documented. Any Irregular Access issues affecting Bright Horizons Information or services shall be reported to Bright Horizons.

Enhanced Level Requirements

13.4. Audit trails of access to Information System housing Bright Horizons Information shall be retained for a minimum period of one (1) year, and shall include any Sensitive Personal Information categories accessed.

14. SOFTWARE AND VIRUS PROTECTION

Basic Level Requirements

14.1. Anti-virus software shall be installed on all Information Systems Processing Bright Horizons Information and updated on a regular basis, having regard to the state of the art and relevant industry best practice. Ordinary users shall not have the ability to turn off the Anti-virus software.

14.2. Contractor shall follow a documented security patching policy, process, and schedule for the infrastructure and layered application products that includes the

assessment of security vulnerabilities and deployment of updates or upgrades in accordance with industry best practice.

14.3. Only licensed copies of commercial software which comply with and do not compromise security standards shall be used.

14.4. The Contractor shall notify Bright Horizons promptly (and in any event within 24 hours of becoming aware) of the actual or potential transmission of any identified computer virus by the Contractor to Bright Horizons.

14.5. No newly acquired discs/media/programmers/executables from whatever source shall be loaded on to Information Systems Processing Bright Horizons Information unless they have been previously vulnerability scanned and virus checked by a suitable vulnerability scanning and virus checking package.

14.6. Appropriate controls to prohibit the download and use of file sharing (e.g. peer-to-peer) and other software that can open security vulnerabilities to Information Systems shall be implemented by the Contractor.

15. SECURITY INCIDENT RECORDING AND RESPONSE

Basic Level Requirements

15.1. The Contractor shall have a documented procedure for identifying, reporting, responding to and managing Security Incidents that affect Bright Horizons Information or Information Systems Processing Bright Horizons Information.

15.2. Recovery of Bright Horizons Information or Information Systems Processing Bright Horizons Information following a Security Incident shall adhere to documented procedures.

16. AUDIT

Basic Level Requirements

16.1. The Contractor shall carry out periodic audits to ensure the ability to comply with these Requirements.

Enhanced Level Requirements

16.2. Information Systems or non-automated means of (i.e. hardcopy filing systems) Processing Bright Horizons Information constituting Personal Information, Sensitive Personal Information, Financial Personal Information, or profiling or depicting the personality or behavior of one or more individuals, shall undergo an internal or external audit at least once every two (2) years to assess their compliance with these Requirements, and the findings delivered in the form of an audit report.

16.3. In addition to this biennial audit, extraordinary audits must be carried out whenever material changes to the Processing are introduced which may affect Bright Horizons Information or Information Systems Processing Bright Horizons Information. The carrying out of any such extraordinary audit will reset the period of two years until the following audit.

16.4. An audit report shall include: a compliance assessment; identify any shortcomings; propose corrective or supplementary measures; and include the information upon which the recommendations are based.

16.5. The Information Security Officer, or other Contractor staff duly authorized in the security document(s), shall analyses the audit report and refer any conclusions to Bright Horizons and the Contractor so that appropriate corrective steps can be taken.

16.6. Bright Horizons shall be permitted access to the audit report and it will be permitted to disclose it to relevant authorities with jurisdiction upon their request where legally required to do so.

17. Vendor and Supply Chain Management

Basic Level Requirements

17.1. The Contractor shall conduct due diligence on its vendors, subcontractors and supply chain in regards to information security.

17.2. The Contractor shall impose same or similar security requirements on its vendors, subcontractors and supply chain that shall have access to Bright Horizons Information commensurate with the data classification.

SECTION 3

MINIMUM REQUIREMENTS FOR TRUSTED CONNECTIONS

1. TRUSTED CONNECTION

In addition to the requirements set forth in Section 2, the following requirements must be met in order to be granted a Trusted Connection and would only apply if triggered by this type of connection. These requirements must continue to be met as long as the Trusted Connection remains in effect. Bright Horizons reserves the right to terminate the Trusted Connection if the Contractor fails to meet the minimum requirements.

1.1. A Trusted Connection shall only be established with a specific Contractor facility. A Trusted Connection established at one secured Contractor facility is not transferable to other Supplier locations or facilities without subsequent approval.

1.2. Physical access to the secured Contractor facility must be restricted to those individuals working for the Contractor on Bright Horizons contracts supported by the Trusted Connection. Any other individuals requiring entry to the facility must be escorted at all times by one of the individuals described above.

1.3. The secured Contractor facility shall provide an isolated network that connects directly to Bright Horizons and does not connect back to the Contractor's own internal network or any other network including the Internet. Internet access will be provided via the Bright Horizons Internet gateways.

1.4. End user computing devices used in the secured Contractor facility shall be either Bright Horizons provided devices with a Bright Horizons Desktop Management Services (DMS) image or Contractor provided devices with a Bright Horizons DMS image. Said devices will be managed and supported in accordance with Bright Horizons supplied processes.

1.5. The Supplier agrees to an initial site survey at the secured Contractor facility and subsequent assessments conducted by Bright Horizons, which includes, but is not limited to, monitoring of the following:

1.5.1. Restricted physical and logical access to devices connecting to the Bright Horizons network;

1.5.2. Connectivity between secured Contractor facility and other networks (including supplier network and the Internet) to ensure that there is no additional connectivity outside of the established Trusted Connection;

1.5.3. End user computing devices to ensure that all are either Bright Horizons machines with Bright Horizons DMS images or Contractor machines with Bright Horizons DMS image, and that all devices will be managed and supported in accordance with Bright Horizons supplied processes.

1.6. The Contractor agrees that Bright Horizons may employ Intrusion Prevention Systems (IPS) or other tools to monitor network traffic or the flow of sensitive intellectual property between the secured Contractor facility and Bright Horizons, specifically to detect malicious traffic on the wire.

SECTION 4

MINIMUM REQUIREMENTS FOR CLOUDS

1. Cloud Utilization

1.1. Bright Horizons' data shall not be stored, processed or transmitted via a cloud service without Bright Horizons' authorization.

1.2. A documented cloud exit plan with secure erasure of Bright Horizons data at contract or previously agreed upon retention period termination shall be in place

1.3. Bright Horizons Highly Confidential data must be encrypted on storage

1.4. Encryption keys shall be stored in a KMS