Rider updated as of 5/17/2021. Use this Rider if the Service Provider will:

- ***Directly plug a computer or other device into a network jack at Harvard;***
- ***Be given credentials (e.g., for HarvardKey or VPN) to access Harvard's non-guest network, wired or wirelessly, or otherwise access Harvard's non-guest network;***
- ***Provide, install, or support any computer or device on a Harvard network.***

This Rider applies to installations and support of hardware and does not apply to installations or support of software only. Note the items to be completed in the first paragraph.

Material changes to these terms must be approved by the University Chief Information Security Officer, except that the encryption requirement in Section 2(vi) can be struck out by the business owner if the Service Provider is unable to meet this requirement.

If the Service Provider will also have access to personally identifiable information, the Service Provider should also sign the Rider on Requirements for the Protection of Harvard Personally Identifiable Information.

Please delete this headnote before transmitting.

Rider:
Requirements for Access to and Protection of
the Harvard Network

Effective as of _____, this Rider is added to and incorporated as part of the *[name of Agreement]* (in this Rider, the "Agreement"), dated as of _____, between *[identify Harvard party]* (in this Rider, "Harvard") and *[identify service provider/vendor]* (in this Rider, "Service Provider"). The requirements set forth in this Rider supplement any other provision of the Agreement requiring the protection of private assets and confidential information. In the event of any conflict between the terms of this Rider and the Agreement, the terms of this Rider shall govern. A definitions section is included at the end of this Rider.

[The following paragraph can be used to replace the introductory paragraph in situations where the Rider is referenced in and incorporated into an Agreement being executed simultaneously. Delete if inapplicable:]

[As stated in the *[name of Agreement]* (in this Rider, the "Agreement"), between *[identify Harvard party]* (in this Rider, "Harvard") and [identify service provider/vendor] (in this Rider, "Service Provider"), this Rider is added to and incorporated as part of the Agreement. The requirements set forth in this Rider supplement any other provision of the Agreement requiring the protection of private assets and confidential information. In the event of any conflict between the terms of this Rider and the Agreement, the terms of this Rider shall govern. A definitions section is included at the end of this Rider.]

1. Any Service Provider Accessing a Harvard Network shall:
   (i) not Access or use, and not allow Access to or the use of, any Harvard Network for any purpose other than the performance of services for Harvard;
   (ii) limit access to Harvard Networks to Permitted Persons;

(iii) ensure that each Permitted Person has a unique individual login to the Harvard Network assigned by Harvard;
(iv) ensure that no Permitted Person shares his/her account, login credentials or passwords; and
(v) notify Harvard as soon as possible and in all events within three (3) business days when a Permitted Person leaves Service Provider's employment or otherwise no longer requires access to any Harvard Network in performance of services for Harvard.

2. Any Service Provider using one or more SP Computers must ensure that all SP Computers meet the following security requirements:
   (i) SP Computer use is limited to the Permitted Person authorized to perform the service via an individually assigned account with password/passcodes that meet the Password Strength Requirements;
   (ii) SP Computer locks after a period of idle time and requires reauthentication of the Permitted Person via their individual password/passcode or biometric identifier to unlock;
   (iii) SP Computer runs a supported and updated operating system;
   (iv) SP Computer runs software with current patches and security updates applied;
   (v) SP Computer runs a supported and updated anti-malware service; and
   (vi) SP Computer uses encrypted storage for data saved to hard drive.

3. Any Service Provider using one or more Devices installed on the Harvard Network by Service Provider or being supported by Service Provider must ensure that all such Devices meet the following security requirements:
   (i) Device is void of any data not pertinent to the contracted service;
   (ii) Device firmware is the most current version provided by the manufacturer;
   (iii) any data required for performance of service is transferred to the Device only after the data has been scanned and determined to be free of known malware;
   (iv) Device is registered according to Harvard-provided settings including Internet Protocol address or range;
   (v) Device is connected only to the Harvard Network and has no other direct connection to other private/public digital, Wi-Fi, Bluetooth, cellular or other network;
   (vi) if a Device has a firewall, (a) the Device firewall rules limit inbound/outbound communication to required ports and authorized services only and (b) any direct connections to embedded management ports from public networks are denied and limited to Harvard's Virtual Private Network or other Harvard-approved remote access solution that requires two-factor authentication;
   (vii) if the Device supports the functionality, (a) Device logs administrator access, including identity of the user, time of activity, and the attempted function (e.g. login or logout) and (b) logs are reviewed at least monthly to determine if there has been any actual or attempted unauthorized access or other unauthorized event affecting any Device or Harvard Network;
   (viii) Device enforces session timeouts and requires reauthentication for administrator access;
   (ix) Device hard-coded credentials are removed, and default accounts are disabled or passwords changed to satisfy the Password Strength Requirements;
   (x) Device requires two-factor authentication for all access, where technically feasible;
   (xi) if the Device supports the functionality, passwords used with the Device are never visible in clear text in storage or transmission;

(xii) any software running on the Device is free of known malware and has all currently available patches and fixes applied;
(xiii) Device maintenance is performed at least quarterly to upgrade firmware and installed software to the most current versions (upgrade and patches) provided by the manufacturer(s);
(xiv) Data transmitted to or from Devices is encrypted in transit where technically feasible; and
(xv) Data removed from Devices to portable storage media must be encrypted at rest.

4. Service Provider must secure an approved exception and compensating controls from Harvard (i) for any requirement in this Rider that a Device or SP Computer does not support or (ii) for any requirement in this Rider the satisfaction of which would materially interfere with contracted services;

5. Service Provider shall notify Harvard as soon as possible and in all events within forty-eight (48) hours upon learning of any event that creates a substantial risk of unauthorized access to, or other unauthorized event affecting, any Harvard Network resulting from or in any way related to a Device or SP Computer, and reasonably cooperate with Harvard in the remediation of such event at Service Provider's expense.

6. Service Provider agrees to comply with such additional protections as Harvard shall reasonably request from time to time in order to comply with any applicable legal requirement.

7. Harvard shall have the right to terminate Service Provider's access to Harvard Networks at any time without notice. At any time on Harvard's instruction and in any case upon termination of the services, Service Provider shall remove all Service Provider Devices and SP Computers from Harvard Networks and shall (unless otherwise required by law) cause all Harvard data on Service Provider's Devices or SP Computers or otherwise in Service Provider's possession in any formats or media to be permanently deleted or destroyed such that it cannot practicably be read or reconstructed.

8. Service Provider shall permit Harvard or an agent of Harvard to conduct an audit at Harvard's expense to ensure compliance with the provisions of this Rider.

9. Service Provider shall provide a copy of this Rider to all its Permitted Persons and enforce and be responsible for compliance by all its employees and contractors with the requirements of this Rider and all security obligations to Harvard.

10. The provisions of this Rider shall survive the termination of the Agreement.

11. For purposes of this Rider:
    (i) "Access" shall mean authorized access to any Harvard Network for the purpose of installing a Device or supporting an installed Device.
    (ii) "SP Computer" shall mean a computer or portable computing device used by or for Service Provider to communicate with Devices directly or remotely (via Harvard Virtual Private Network or other Harvard-approved remote access solution that requires two-factor authentication).

(iii) "Device" shall mean a computer or other device installed and resident on a Harvard Network.

(iv) "Harvard Network" shall mean (i) any set of directly or remotely connected services and communication facilities managed directly or via contract by or for Harvard, including two or more devices with capability to monitor, control, and/or transmit data among them through communication facilities, and (ii) any servers operated by or exclusively for Harvard.

(v) "Password Strength Requirements" shall mean the following requirements for passwords:

1) no common names or dictionary words, unless part of a multi-word phrase with no spaces;
2) at least one character from three of the following categories: uppercase letters, lowercase letters, numbers, special characters; and
3) one of the following requirements: (i) minimum of ten characters, (ii) minimum of eight characters and at least annual password reset or expiration, or (iii) minimum of eight characters and a second authentication factor.

(vi) "Permitted Person" shall mean a Service Provider's employees and contractors who have a specific need for access to Harvard Networks in order to perform Service Provider's services for Harvard.

[The following signature block can be removed in situations where the Rider is referenced in and incorporated into an Agreement being executed simultaneously.]

For Service Provider	For Harvard
By_____	By_____
Name:	Name:
Title:	Title:

[The following provision should be added if there are specific technology configurations – insert the following after section 3 (and renumber sections as appropriate). Delete if inapplicable:]

4. The Service Provider shall ensure that any Device or SP Computer that accesses a Harvard Network complies with the following technology configurations:

[Add specific configurations]