Service Provider / External Hosting Services

Security Checklist

The Service Provider / External Hosting Services Security checklist applies to situations where Bryant University is considering an external hosted service such as an application service provider (ASP) or a software-as-a-service (SaaS) provider.

Applications and services hosted by externally hosted services bring special security challenges. A security assessment or review is required to be conducted if any of the following apply to the project:

1. The project involves transferring any university data classified as **Confidential or Private**, or otherwise sensitive, from a university-owned device to a third-party contracted device.
2. The project involves contracting with a vendor who will create a network-accessible service on behalf of Bryant University to collect, transmit, or process any university data classified as **Confidential or Private**, or otherwise sensitive.
3. The project requires that a contracted third party collect or process any university data classified as **Confidential or Private**, or otherwise sensitive, that will later be transmitted for use by Bryant University.
4. The project requires that a third party process payment card information on behalf of Bryant University.

It is the responsibility of the application owner or data steward to confirm the correct data classification category of the project. See Data Classification Guidelines.

The ability of Bryant University to service its students, manage its costs and meet its regulatory requirements may be affected by the products, services, and systems that are hosted by third party providers. In selecting a host provider, it is important to take into consideration many factors, such as strategic purpose, business objectives, benefits, legal requirements, costs, needs, financial stability, performance capabilities and technical and operational requirements.

This checklist is a guide for evaluating the security of an external hosting service that will be providing hosting services for the University.

Outsourcing or Hosting Services Security Checklist

Section I.

To be completed by Bryant University application owner or data steward

	Yes	No	Comments
1. Is any of the data to be maintained by the host provider subject to federal regulations such as HIPAA, FERPA, or GLBA?			
2. Is any of the data to be maintained by the host provider subject to Payment Card Industry (PCI) Data Security Standards?			
3. Is any of the data to be maintained by the host provider classified as Confidential or Private as defined by the University Data Classification Guidelines and not already identified in questions 1 and 2?			
4. Are appropriate signed agreements in place? Specifically, has a contract been signed that specifically enumerates the duties of the provider in regards to access, restriction of use, return of confidential information, sharing of audit findings, subcontracting, and security breach disclosure?			
Contract/Agreement signed date(s)			

Section II:

To be completed by Service or Hosting Provider:

Please provide a Yes, No, or n/a to each question. If a question is answered with a No or n/a, please provide additional information in the Comments section.

(Note: If the vendor is a member of the "Cloud Security Alliance" (CSA), they may option to submit a completed "Cloud Controls Matrix" in place of or in addition to completing Section II if you have completed a SOC 2 (Service Organization Control) portion of the SSAE 16 standard (Statement on Standards for Attestation Engagements), you are encouraged to submit your SOC 2).

	Yes	No	Comments
1. Does your organization have a documented and provable internal information security policy in place that detail your information protection program for both logical and physical security? (List of items in security policy: organization structure, physical security, hiring and termination procedures, data classification, access control, operating systems, Internet use, email and virus protection, firewall, VPN, remote			

access, backup and disaster recovery, personnel security, software development)			
2. Is this policy reviewed and updated on a regular basis?			
3. May a copy of your information protection program be reviewed by Bryant University?			
4. In order to protect the confidentiality, integrity, and availability of Bryant University's's confidential information, does your organization ensure that:			
a. Information and services are provided only to those authorized?			
b. The information is protected so that it is not altered maliciously or by accident?			
c. Information and services are provided in conjunction with the vendor's disaster recovery and business continuity planning policy?			

	Yes	No	Comments
6. Are backup/recovery procedures updated and tested annually?			
7. What type of testing do you conduct for your business continuity and disaster recovery plan (i.e. simulation drills, walk-through exercises, tabletop exercises, actual drills, etc)?			
8. What is the frequency?			
9. How long do you estimate it will take to restore a product or service should you experience a serious business interruption that lasts more than 1 business day?			
10. Is access to offline media and backup data restricted to authorized individuals only?			
11. Are physical security measures in place to protect Bryant University data from modification, disclosure, and destruction?			
12. Does your organization use a co-location facility for housing your servers?			
13. If a co-location facility is used:			
a. Does co-location facility provide physically secure "apartments" or cages for each tenants' equipment?			
b. Are the server racks/cage area locked?			
c. Are the servers kept in an area with access restricted to authorized personnel?			

d. Are monitoring and surveillance solutions implemented?			
14. Are servers protected by environmental controls (smoke detectors, fire suppression systems, water sensors, uninterruptible power supplies (UPS), and temperature sensors?			
15. Are all visitors required to sign a security log and be accompanied by an escort while in production areas?			
16. Does your organization have an Information Security Administrator function separate from a System Administrator function?			
17. Are annual external audits performed on the physical and information security controls?			
18. When was the last audit performed?			
19. Can a copy of your most recent external audit report be provided to Bryant University for review? (i.e. SSAE16 SOC 1, SOC 2 or SOC 3 audit report, external audit report and/or executive summary of audit) ** For PCI, please include documentation showing a recent PCI audit			
20. Do you log unauthorized attempts to the system and application?			

	Yes	No	Comments
21. Do you preserve event logs in case of a breach or investigation?			
22. Are logs kept in a central location, separate from the system components?			
23. How long are logs retained?			
24. Does your organization use a local Intrusion Prevention System(s) IPS?			
25. Does your organization use a local Intrusion Detection System(s) IDS?			
26. Are procedures in place for reporting and responding to possible security incidents?			
27. Do you have a separate development environment from your production environment?			
28. Is there a separate test environment?			
29. Are documented change control procedures in place?			

30. Are logical security measures in place to protect Bryant University's data from modification, disclosure, and destruction?			
31. Will Bryant University's data be securely segregated from the data of other customers?			
32. Will encryption be used on any of Bryant University's data? If YES, please indicate the encryption to be used and where in the *Comments* field.			
33. Who will have access to Bryant University's data?			
34. When are they authorized to handle/view our data?			
35. Where is the data being stored? List all geographic locations that will apply. (e.g. Northern California, Northern Virginia, Europe)			
36. Who holds ownership of the data once stored at your location(s)?			
37. Who will handle the administration of the users in the application?			
a. Bryant University			
b. Provider			
38. Does your organization enforce a strong password policy?			
39. Are your employees/contractors required to sign a confidentiality agreement?			
40. Do you have a mandatory security awareness program in place for employees to make them aware of confidential information, the company's security policies and standards and good security practices?			
41. Are reviews conducted to validate that user access is appropriate? (i.e. inactive accounts, employees who have changed job responsibilities or who have terminated employment)			
a. What is the frequency?			
i. Monthly			
ii. Quarterly			
iii. Annually			
iv. Semiannually			

	Yes	No	Comments
42. Do you immediately disable or modify access entitlements when an employee's status changes (termination, transfer, etc.)?			
43. Is there a documented process to verify a requestor's identity and the need-to-know before access is given to Bryant University's information?			
44. Do you apply security patches on a regular basis? If YES, please indicate the frequency in the *Comments* field.			
45. Do you have a defined process for testing and applying critical patches outside of your regular patch cycle?			
46. Is the appropriate anti-virus software employed and regularly updated?			
47. Is penetration testing conducted annually to determine vulnerability of network and to determine the level of damage that could occur if compromised?			
48. Do you outsource any processing to another third party provider?			
49. If yes, list the names of the outsource provider(s)			
50. If outsourcing is done, are any of your outsourced providers' facilities located outside of the United States? If YES, please list countries in the *Comments* field.			
51. Do you have a privacy policy to prohibit the sharing of customer information, except as allowed by privacy legislation exceptions?			

Provider Information:	
Completed By:	
Title:	
Date:	
Contact Information:	