Security Requirements for Non-Microsoft Hosted Facilities

|  |
| --- |
| **This contract exhibit is used for Third Party Channelizer, XML Feeds, iFrames and Video Content that host services in non-Microsoft facilities.** |

**Introduction**

The **Security Requirements** section describes the hosting environment and co-branded site requirements that ensure alignment with Microsoft online security policy and standards.

1. Complete Table 1 of this exhibit to provide required third party site registration information.
2. Email a PDF version of the signed contract that includes the completed Security Requirements Exhibit to the [CPRM@microsoft.com](mailto:CPRM@microsoft.com) alias to initiate the registration and scan authorization for the third party site.

**NOTE:** Submissions of a Security Requirements exhibit that is not included as part of a signed contract requires the partner to authorize site scanning by signing a Scan Compliancy Form. Both the Security Requirements exhibit and signed Scan Compliancy form should then be submitted to the [CPRM@Microsoft.com](mailto:CPRM@Microsoft.com) alias.

**Table 1: Co-Branded Site Registration Information**

|  |  |  |
| --- | --- | --- |
| **PARTNER INFORMATION** | | |
| **1** | **Partner Name** | **Omrop Fryslân** |
| **2** | **Partner Country** | **Netherlands** |
| **3** | **Partner Region** | **EMEA** |
| **SITE INFORMATION** | | |
| **4** | **Microsoft Service**  *MSN, Windows Live, Bing, Other* | **MSN** |
| **5** | **Host IP Type**  *Static or Dynamic* | Choose an item. |
| **6** | **Hosting Platform**  *Microsoft, non-Microsoft, mixed platforms* | Microsoft |
| **7** | **Microsoft Co-branded Site Hosting Provider**  *Name of Hosting Provider* |  |
| **8** | **Microsoft Co-branded URL(s)** | < your NewsML feed URL here > |
| **9** | **Microsoft Co-branded IP(s)** | < the IP address of your webserver here > |
| **10** | **Data Classification**  *High Business Impact (****HBI****; Moderate Business Impact (****MBI****);*  *Low Business Impact (****LBI****); Microsoft Business Development team members can obtain data classification assistance via* [*http://ignition/assetclassificationwizard*](http://ignition/assetclassificationwizard) | **Low Business Impact** |
| **11** | **Business Value**  *Data hosted on behalf of Microsoft must be designated into one of three business classification (****Low, Medium, High****) by the Business Development team.* | **Moderate Business Value** |
| **CONTRACT INFORMATION** | | |
| **12** | **Contract Start Date** | **7/1/2012** |
| **13** | **Contract End Date** | **6/30/2013** |
| **ESCALATION INFORMATION** | | |
| **14** | **Partner Primary Business Contact**   * **Name** * **Email** * **Phone** | Sybren Terpstra |
| Sybren.Terpstra@omropfryslan.nl |
| +31582997775 |
| **15** | **Partner Technical Contact**   * **Name** * **Email** * **Phone** |  |
|  |
|  |
| **16** | **Microsoft Primary Business Contact**   * **Name** * **Email** * **Phone** | Brendan Thesingh/Davina Bos |
| [brendant@microsoft.com](mailto:brendant@microsoft.com) [davinab@microsoft.com](mailto:davinab@microsoft.com) |
| +31205001946 +31205001572 |
| **17** | **Microsoft Country Manager**   * **Name** * **Email** * **Phone** | Theo Rinsema |
| [theor@microsoft.com](mailto:theor@microsoft.com) |
| +31205001147 |
| **18** | **Microsoft Security Incident Escalation Contacts** | [**MOCAlert@microsoft.com**](mailto:MOCAlert@microsoft.com) **(and)** [**WLSIM@microsoft.com**](mailto:WLSIM@microsoft.com) |
| **19** | **Microsoft Availability Issue Escalation Contact** | [**LSEPartner@microsoft.com**](mailto:LSEPartner@microsoft.com) |

**SECURITY REQUIREMENTS**

The following summarize the minimum security requirements for Third Party Partners that provide Microsoft co-branded sites and services. Some of the content in this exhibit is technical in nature therefore third party partners should engage appropriate technical staff to verify the company’s ability to comply with the stated security requirements. Any questions regarding any of the requirements below can be directed to [CPRM@microsoft.com](mailto:CPRM@microsoft.com).

**Service Level Requirements**

# Service Level Scope

The Third Party Partner shall be the primary interface with Microsoft. Management of sub-contracted parties that enable the support of the co-branded site is the responsibility of the Third Party Partner. Parties will conduct business in English for all communications relating to this agreement.

Third Party Partner shall be responsible for those aspects, components, inputs, and interfaces of the content solution or software development that fall directly under the control of Third Party Partner infrastructure and personnel up to the Service Border.

If Third Party Partner does not directly host or develop the co-branded site, Third Party Partner shall include the conditions defined in the Security Requirements Exhibit in its agreement(s) with the hosting facility.

**Minimum Security Requirements**

The following sections align with Microsoft online security policy and standards as it relates to third party hosting environments and development of secure co-branded sites on behalf of Microsoft.

# Security Policy Compliance

To ensure data security, confidentiality, integrity and availability of co-branded sites, third party partners that provide co-branded site development and hosting services on behalf of Microsoft must apply the minimum security requirements as described in this exhibit.

If Microsoft reasonably requests that Third Party Partner employ additional security procedures or requirements and the parties are unable, after good faith negotiations to agree upon the terms of such implementation, then Microsoft shall have the right to terminate this Agreement by providing written notice to the Third Party Partner.

In addition to the requirements defined in this exhibit the Third Party Partner is also responsible for complying with all applicable statute, policy, regulation and industry standards that may apply to this contract (e.g. PCI compliance for credit cards, etc.)

# Data Classification Requirements

To ensure appropriate security controls are applied, Third Party Partners that develop and/or host co-branded sites on behalf of Microsoft are required to provide Microsoft with site information that enables assignment of the appropriate data classification that represents the ‘highest value’ of the data being handled by the co-branded site. Detailed descriptions of data classification are found in the following sections of this exhibit.

|  |  |  |
| --- | --- | --- |
| **Data Classification** | **Classification Summary** | **Section** |
| Low Business Impact (LBI) | Publicly available content such as news media or public keys | 12 |
| Moderate Business Impact (MBI) | Information assets that are intended for limited use by specified groups, such as, name or address | 13 |
| High Business Impact (HBI) | Information assets that could be used to authenticate or authorize valuable transactions, such as financial data or government issued identification | 14 |

Failure to assign the appropriate data classification may result in site shutdown until appropriate scans can be performed to verify security controls are in place.

# Security Policy/Program

Third Party Partner represents and warrants that it maintain and will continue to maintain an information security policy or program that defines the protection requirements and mechanisms to ensure the security, confidentiality, integrity and availability of data assets.

Microsoft reserves the right to review Third Party Partner’s security policy, program and hosting facility for compliance with Microsoft online services policy and standards.

# Secure Development Requirements

Third Party Partner should apply industry best practices, such as Security Development Lifecycle (SDL) for secure development to protect the co-branded site and customer records from at least, but not limited to the following security vulnerabilities:

* Cross site scripting
* Injection attacks
* Credential or customer data loss
* Cross site request forgery
* Broken authentication and session management
* Insecure cryptographic storage

Failure to develop a secure co-branded site may require site redesign to meet minimum security requirements and result in site launch delays or site shutdown.

# Source Code Management

The Third Party Partner must protect the source code of the co-branded site application it develops for Microsoft so that it is inaccessible to other parties. The source code must be saved on a protected centralized server with full backup features. Access history of the source code should be kept for at least 30 days for audit purposes.

# Capacity Planning and Management

At the time of launch, Microsoft expects that the service is ready for and can meet the demands of the [Peak Traffic] calculation + 25%. The Third Party Partner must ensure that the service can meet the Peak Traffic demands throughout the life of the contract.

# Cryptography Requirements

Co-branded sites that use cryptography to protect client-side data should use only Microsoft standard cryptographic libraries. It is expected that all development will be undertaken using Managed Code and should use the System Security Cryptography namespace and its classes to provide all cryptographic services.

The following table details the current Microsoft recommended crypto-algorithm implementations and key lengths, which may be updated by Microsoft from time to time. Any implementation of cryptography should adhere to these guidelines.

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm Type** | **Algorithm** | **Key Length** | **Notes (Classes/Namespace)** |
| Symmetric Block | AES | >=128 bit | RijndaelManaged |
| *Symmetric Stream* | *N/A* | *N/A* | *Block cipher should be used* |
| Asymmetric | RSA | >=2048 bit | RSACryptoServiceProvider |
| Diffie-Hellman | >=2048 bit | Pkcs Used for key agreement |
| ECC | >=256 bit | Natively supported in Vista but a managed code library will not be available until the next Visual Studio release, 2007/2008. |
| \* Hash (inc MAC) | SHA-256 | 256 bit | SHA256Managed, HMACSHA256 |
| SHA-384 | 384 bit | SHA384Managed, HMACSHA384 |
| SHA-512 | 512 bit | SHA512Managed, HMACSHA512 |
| HMAC Key Lengths |  | >=128 bit | HMAC is keyed hashing for message authentication. It makes use of an underlying hash and a secret key of a specified length. |

\* All other hash functions, including MD2, MD4 and MD5 must not be used as they have a demonstrated vulnerability to collision attacks.

**NOTE: Custom cryptographic implementations may not be used under any condition.**

# Domain Names and DNS

All domain names which are associated with a Microsoft brand should be registered and managed by Microsoft.

# Security Scan Requirements

Co-branded sites and hosting environments are required to be scanned by Microsoft to ensure the site is reasonably free of security vulnerabilities, both pre- and post-launch. At time of registration Microsoft will provide Third Party Partner with minimum scanning requirements and post-launch scan schedule.

Third Party Partner is required to advise Microsoft when updates to server host configuration and co-branded web applications have the potential of altering existing levels of security. Microsoft will conduct a rescan to ensure site security levels are appropriate.

## Pre-launch Scan Requirement

Microsoft scanning services will conduct pre-launch scans within three business days of registration. The scan scope aligns with the following table:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Business Value** | | |
| **Data Classification** | **Low** | **Medium** | **High** |
| LBI | Host Scan | Host Scan | Host and Application Scan |
| MBI | Host Scan | Host and Application Scan | Host and Application Scan |
| HBI | Host and Application Scan | Host and Application Scan | Host and Application Scan |

## Post-launch Scan Requirement

Microsoft scanning services will conduct periodic post-launch host configuration scans for the duration of the contract to ensure co-branded sites remain secure. Microsoft will provide notification prior to conducting post-launch scans. The scope of the scans will be in alignment with the following table:

|  |  |
| --- | --- |
| **Data Classification** | **Scan Schedule** |
| LBI | Quarterly |
| MBI | Monthly |
| HBI | Bi-monthly |

## Scan Permission and Access

Third Party Partner grants Microsoft legal permission to perform necessary pre-launch and post launch scanning for co-branded host servers and web applications as part of this contract to ensure the site security levels meet Microsoft minimum requirements. Permission is granted by executing the contract in which this exhibit is attached.

To facilitate the host configuration scanning Microsoft requires hosting providers to whitelist Microsoft scanning tool IP addresses in perimeter devices to facilitate vulnerability detection. Third Party Partner will arrange for such whitelisting of Microsoft’s scanning tool IP addresses. Temporary authentication credentials may also be required to be created by the Third Party Partner to enable web application scanners to test the co-branded site for common security vulnerabilities related to site code, and Third Party Partner agrees to provide necessary authentication credentials upon Microsoft’s request. Third Party Partner will comply with any other reasonable requests by Microsoft for information and access to conduct necessary scans to ensure co-branded site security.

Upon termination of the Content Level Agreement, Third Party Partner shall remove whitelisted IP addresses for Microsoft scanners from perimeter devices.

* 1. **Vulnerability Remediation**

Microsoft scanning services will provide the Third Party Partner with scanning results each time a scan is performed. Third Party Partner is required to remediate identified vulnerabilities within the following time frames.

* Vulnerabilities found as part of a co-branded site pre-launch scan must be remediated by the Third Party Partner prior to the site go-live.
* Vulnerabilities found after a co-branded site has launched are required to be remediated by the Third Party Partner within the timeframes provided in the notification, or as otherwise agreed upon in writing with the Microsoft.

# Security Incident Response and Remediation Requirements

* 1. **Security Incident Detection**

Third Party Partner shall report as soon as feasible any actual or suspected threats to the security of sensitive information, or any material weakness that could allow unauthorized access to sensitive information related to the co-branded site.

Third Party Partner shall take appropriate steps to mitigate the threat, and the parties shall mutually agree on appropriate further steps to alleviate any continued threat and prevent foreseeable future threats to the security or privacy of sensitive information.

## Third Party Partner is required to promptly escalate security incidents to [MOCAlert@microsoft.com](mailto:MOCAlert@microsoft.com) and WLSIM@microsoft.com.

* 1. **Security Incident Notification, Response and Site Shutdown**

## Third Party Partner will be notified of security incidents and related vulnerabilities identified by or reported to Microsoft. Third Party Partner is required to acknowledge receipt of security incident notifications within three business days.

## Third Party Partner must mitigate and remediate security issues related to incidents in alignment with the following table or as otherwise agreed upon with Microsoft.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Rating** | **Mitigation Timeline** | **Remediation Plan Presented to Microsoft** | **Remediation Requirement** | **Examples** |
| **Critical** | Immediate | 24-48 hours | QFE/Hotfix | Any code flaw that could threaten the survival of the business, either through service impact, or exposure of sensitive data. |
| **High** | 4 hours | One week | QFE/Hotfix | SQL injections that are publicly known XSS attacks actively exploiting users |
| **Med** | 1 business day | 30 days | Next release | Publicly known XSS attacks.  Internally reported SQL injections |
| **Low** | 2 business days | 30 days | Next major release | XSS vulns reported responsibly to MSRC |

## Failure to acknowledge receipt of an incident, provide a remediation plan or closure of identified vulnerabilities reported by Microsoft to the Third Party Partner may result in the third party site being shut down by cloaking the DNS until the identified security issues are remediated.

* 1. **Compromised Site Response**

In the event of a security compromise or breach Third Party Partner, its employees, agents and contractors must ensure all data from affected system(s) is retained and stored in a manner that protects the confidentiality, integrity and availability of such data until a thorough assessment can take place. Compromise response documentation and electronic data must be handled in a manner that supports chain of custody.  Microsoft, its affiliates, and law enforcement agencies shall be permitted access to review forensics data, as appropriate to assist in the response and remediation efforts.

# Co-branded Site and Hosting Environment Technical Security Requirements for LBI Sites

Information assets not falling into either the *High Business Impact (HBI)* or *Moderate Business Impact (MBI)* are classified as *Low Business Impact (LBI)* and have limited protection requirements. These information assets are typically intended to be widely published information where unauthorized disclosure would not result in any financial or material loss, legal or regulatory violations, operational disruptions, or competitive disadvantage to Microsoft or relying parties.

Some examples of *LBI* assets include but are not limited to:

* Publicly accessible web pages
* Public cryptographic keys
* Published press releases, product brochures, white papers, and documents included with released products
  1. **LBI Network Requirements** 
     + Internet facing publicly accessible servers must be protected via router access control lists (ACL’s). An allowed port list or firewall configuration should be supplied by those responsible for the firewall maintenance before deployment.
     + Allow only appropriate external protocols. For most cases, only TCP port 80 and 443 should be open to Internet with all other TCP or UDP ports closed.
     + FTP, Mail Services and/or other file transfer protocols should never be open to Internet without IP restrictions set to trusted partner sources. It should by default deny ALL connections with whitelist exceptions only.
     + SSH, Terminal Services, Database Services and/or other Administration protocols should never open to Internet without IP restrictions set to trusted administration sources. It should by default deny ALL connections with whitelist exceptions only. The sessions are required to be encrypted always.
     + Network IP ranges must be logically segmented from non-Microsoft co-branded site related systems. This typically requires network level ACLs to be in place to ensure only trusted and mission-related systems can communicate with the co-branded server.
     + External network resources such as access to monitoring or administrative web sites must be locked to specific IP addresses to decrease the exposed attack surface.
  2. **LBI Operating System Requirements** 
     + Co-branded servers must have virus scanning software for system partitions, including a real-time memory resident scan if the Operating Systems supports (Windows systems are always required to have anti-virus solutions). Data partition scanning is required if the server delivers files to clients directly, this can be configured and confirmed on the source of those delivered files. (Unix-based servers are exempted from this requirements)
     + Telnet must be disabled or uninstalled on Windows and Unix installations.
     + Servers must implement appropriate security operations mechanisms, including security patches, hot fixes, system configurations and a documented software update process.
     + Operators must have unique accounts for administrative access. No other accounts should reside on system. The GUEST account must be disabled for Windows Operating Systems.
     + Unnecessary services must be disabled.
     + Passwords must have a minimum length of 8 characters; contain at least 2 alphabetic characters and at least one numeric or special character.
     + There must be a password change process for all accounts, including administrative and service passwords and should be enforced by documented or domain policy.
  3. **LBI Web Server Requirements** 
     + Transfer protocols are not installed for public usage.
     + Web servers should have a documented log management policy clearly defining the following.
  + Number of days for which log is stored on the servers
  + Number of days for which archived log is available
  + Web Server (along with its components) and its operating system should be on current vendor supported version and always have the latest security patches installed. Web server on Microsoft version should have the latest (or N-1) service packs installed.
    - SSL certificates and/or any other type of certificates should support at least 128-bit strength and only use strength with 128-bit or above. SSLv1 and SSLv2 should not be used.
  1. **LBI Database Server Requirements** 
     + Database server, including components relevant to the co-branded site and its operating system should be on current vendor supported version and always have the latest security patches installed and should be no less than N-1. Where N is the latest version / patch set from the installed release.
     + Passwords for the system administrator and system users must be changed from default following the strong password structure.
     + Applications must not log in to database server for query using the admin privileged accounts (e.g. SA in SQL Server).
     + Applications must log into database server with a unique account containing only the permissions that the application needs to write or read to the Database.
     + Database must be configured in archive log mode to facilitate point-in-time recovery in case of database server crash if the database engine supports.
     + At a minimum, daily backups must be performed for databases related to co-branded sites.
  2. **LBI Web Application Security**
* Application\* must be designed and tested to avoid Cross Site Script Issues.
* Application\* must be designed and tested to avoid SQL Injection Issues.

\* Application: referred to scripts, pages, executable code, components running on the server or downloaded to the client PC).

* 1. **LBI Physical Security Requirements**
* Servers and devices hosting LBI data or providing co-branded site functionality are required to be secured from unauthorized physical access.
  + - * + Third Party Partner will conduct quarterly audits of access levels assigned to electronic access control equipment (i.e. card readers) allowing access into rooms housing servers and make appropriate changes.
    - The Hosting Facility should have video cameras in place to capture and record images of activity at hosting floor entries and exits, as well as at all hosting facility perimeter entries and exits.

# Co-branded Site and Hosting Environment Technical Security Requirements for MBI Sites

Moderate Business Impact (MBI) relates to third party partner sites that handle limited types of customer information assets that cannot be used to directly or indirectly represent an individual customer, authenticate or authorize valuable transactions.

* All Personally Identifiable Information (PII) that is not listed as Highly Sensitive PII. MBI includes but is not limited to information regarding: an individual’s race, ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, and/or commission or alleged commission of offenses and court proceedings. This category also includes information that can be used to contact an individual such as name, address, e-mail address, fax number, phone number, etc.

All Private cryptographic keys used for encrypting data are to be classified as MBI.

## Moderate Business Impact (MBI) Requirements include LBI requirements plus the following set of requirements.

* 1. **MBI Data Requirements**
* Access to Microsoft data must be limited only to those individuals who require the specific data in the course of their regular, documented duties.
* Access controls around Microsoft data must be audited on a quarterly basis to ensure continued data protection.
* All Microsoft MBI data must be encrypted while in transit. This usually requires HTTPS protocol for pages that collect MBI data from end users.
* Co-branded sites using a Microsoft owned domains must obtain the digital certification public key and private key from the Microsoft designated group.
* Encryption should be equal or stronger than 128 bit.
  1. **MBI Network Requirements**
* Strict network level ACLs are required to be in place so that only trusted and mission-related system can communicate to the co-branded server that host PII data.
  1. **MBI Operating System Requirements**
* Applications and services must be run using the least privilege required for operation.
  1. **MBI Web Server Requirements**
* Default web server (for example, Apache or PHP) installed directories should be removed.
* Session keys or PII data should never be sent over as URL parameters. Cookies with encryption are to be used to prevent unauthorized disclosure of PII data.
* With the exception of .NET mappings all unnecessary IIS extensions should be removed from the default configuration. .NET mappings (aspnet\_isapi.dll) should remain untouched even if the file type is not in question. With few exceptions, IIS must not run on the same box as SQL. Exceptions where SQL and IIS can coexist on the same server:
  + Test environments that do not contain user/customer PII including but not limited to email address, PUID, name, address, phone number, password, user name or credit card information.
  + One physical server running multiple virtual machines where one VM has SQL installed and another VM has IIS.
  + Back-end machines that are not directly accessible from the Internet (do not have an externally routable IP).
  + Default IIS install (vdirs, scripts and samples) directories created by the installation should be removed. All content in the directories must be removed and the default web site should not be used.
  + The web server is operated under a non-privileged account.
  1. **MBI Database Server Requirements** 
     + - Database Engine and supporting components (for example: SQL or SQL Agent) are not to be operated with elevated privileged accounts.
       - Cross-Server Database Remote Access must not be enabled. For example, in SQL Server, SQL Remote Access (Sp\_configure “remote access”) must be set to 0.
       - Database must be configured to log security events such as login / logout and failures to the event log.
       - Database Engine Installation log files should be removed. For Microsoft SQL Server, the log files contained at c:\windows\setup.iss and sqlsp.log must be deleted since it contains the passwords used in setup.
       - Database Server must not be directly exposed to the Internet.
       - If Microsoft SQL Server is used, it should listen only on TCP or Named Pipes. To prevent issues with other protocols or unexpected conflicts, only the two protocols listed above should be used.
       - Non-administrator accounts must not be able to execute commands directly on the database server. For Microsoft SQL Server, non-administrator accounts must not be able to execute CmdExec functions.
       - Applications must not use system functions that can run command line instructions. For example xp\_cmdshell in Microsoft SQL Server. Xp\_cmdshell is similar to the CmdExec functions and should not be used for the same reasons.
       - Application must be authorized only for the tasks that are needed to host the co-branded site.  To enforce this requirement, the database must have unique roles defined on a per authorization list basis.
       - Default access to the database tables for all users (like all\_users, db\_users in SQL Server) should be restricted.
       - Database servers must have disaster recovery plan that includes events such as system crash or physical damage. Tape backup is the minimal requirement of a disaster recovery plan.
  2. **MBI Physical Security Requirements**
* Only electronic access control systems will be used to provide access to rooms or cages that host Microsoft MBI level servers.
  + - * + The Third Party Partner or Hosting Facility will conduct quarterly audits of access levels assigned to electronic access control equipment (i.e. card readers) that control access into rooms housing Microsoft MBI level servers.
        + All perimeter walls of rooms housing Microsoft MBI servers will extend from the concrete flooring to the concrete roof (“slab to slab”) and not stop at a drop, lowered, or false ceilings, or at raised floors allowing someone to climb over or under to gain access. All perimeter walls will have no openings larger than 12 inches in width or height that are not covered by properly secured protective screening, fencing or vents. Cages must also conform to the same parameters.
    - All co-branded servers must be located inside a locked rack. The rack access doors and panels must be kept closed and locked when personnel are not actively working inside the rack.
    - No entries or openings on the rack’s front, back, sides, top, or bottom will be large enough to allow a media device or cable connection to be passed through and attached to the hardware stored in the rack, unless done from inside the rack by authorized users per policy.
    - Rack keys will be held by the Third Party Partner or Hosting Facility designated personnel. Logs of who signs out or uses the rack keys will be maintained for 90 days. The logs will contain enough information to clearly record the identity of the individual. Key requestor’s identity must be confirmed by valid government issued photo identification by authorized partner or hosting provider personnel.
    - The Hosting Facility must have video cameras in place to capture and record images of activity at hosting floor entries and exits, as well as at all hosting facility perimeter entries and exits.

# Co-branded Site and Hosting Environment Technical Security Requirements for HBI Sites

This classification includes data assets that could be used to directly or indirectly authenticate or authorize valuable transactions such as:

* Authentication/authorization credentials (i.e. username/password pairs, private cryptographic keys used for authentication/authorization or numeric identification sequences such as PINs, and hardware or software tokens).
* Information assets subjected to specific regulatory requirements (i.e., under local law)
* Highly Sensitive Personally Identifiable Information (HSPII) which includes:
  + Government-provisioned identification credentials (e.g. social security or driver’s license numbers)
  + Financial transaction authorization data (e.g. credit card number, expiration date and card ID
  + Financial profiles (e.g. consumer credit reports or personal income statements)
  + Medical profiles (e.g. medical record numbers or biometric identifiers)

Information in this class is intended strictly for limited business use on a “need-to-know” basis only. The number of people with access to this data should be small and strict rules in the usage and handling of this data must be adhered to. Access must be strictly monitored and controlled at all times.

## High Business Impact (HBI) Requirements include LBI and MBI requirements plus the following set of requirements in this section.

* 1. **HBI Data Requirements** 
     + All Microsoft HBI data must be encrypted while in transit and while stored and not in use.
     + All Microsoft HBI data must be secured using two distinct authentication mechanisms as shown following examples.
       - What is known by an individual to validate identity such as passwords and PINs
       - What is in possession by an individual to validate identity such as electronic keycards
       - Unique features of an individual that is used to validate identity such is retinal or fingerprint scans
     + Physical access to HBI data must be secured.
  2. **HBI Network Requirements** 
     + Network has alerting in place to recognize and report unauthorized access.
     + All network wire and cable supporting the transmission of Microsoft HBI data must be routed through secured Third-party Hosting Facility space. Any cable that must cross outside of the secure perimeter must be installed in rigid metal conduit only with no access points outside the secure perimeter; this includes all ingress and egress connectivity to the Third-party Hosting Facility.
  3. **HBI Web Server Requirements**
     + If using Microsoft platform, all IIS Servers should use Windows Authentication to connect to SQL Server.
     + Web application should use 2-way authentication API when it calls other application server, web server or database servers and send/receive HBI data.
  4. **HBI Database Server Requirements** 
     + BUILTIN/Administrators must be removed from the Database Administrative group (if the system by default set these roles).
  5. **HBI Web Server Requirements**
* All IIS Servers use Windows Authentication to connect to SQL Server.
  1. **HBI Database Server Requirements**
* BUILTIN/Administrators must be removed from the SQL Administrative group.
  1. **HBI Physical Security Requirements** 
     + Only electronic access control systems will be used to provide and control access to rooms or cages that host Microsoft MBI or HBI level servers.
     + The Third Party Partner or Hosting Facility will conduct quarterly audits of access levels assigned to electronic access control equipment (i.e. card readers) allowing access into rooms housing servers and make appropriate changes.
     + All perimeter walls of rooms housing servers will extend from the concrete flooring to the concrete roof (“slab to slab”) and not stop at a drop, lowered, or false ceilings, or at raised floors allowing someone to climb over or under to gain access. All perimeter walls will have no openings larger than 12 inches in width or height that are not covered by properly secured protective screening, fencing or vents. Cages must also conform to the same parameters.
     + All servers must be located inside a locked rack. The rack access doors and panels must be kept closed and locked when personnel are not actively working inside the rack.
     + No entries or openings on the rack’s front, back, sides, top, or bottom will be large enough to allow a media device or cable connection to be passed through and attached to the hardware stored in the rack, unless done from inside the rack by authorized users per policy.
     + Rack keys will be held by the Third Party Partner or Hosting Facility designated personnel. Logs of who signs out / uses the rack keys will be maintained by the Hosting Facility for 90 days. The logs will contain person’s printed name, signature of the person, person’s company name, key number, property name, rack location, date keys signed out, time keys signed out, time keys signed in, date keys signed in, initials of the person receiving the keys. Key requestor’s identity must be confirmed by valid government issued photo identification.
     + The hosting facility must have video cameras in place to capture and record images of activity at hosting floor entries and exits, as well as at all hosting facility perimeter entries and exits.

**Security Requirements Terminology and Definitions**

**The terms of this Service Requirements are defined using industry standard definitions based on Information Technology Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF).**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Co-branded Site** | Site that is owned by a non-Microsoft company but contains Microsoft branding |
| **Content Partner Risk Management** | Microsoft service that governs the engagement for third party co-branded sites and services. |
| **Critical Service** | Service that if interrupted and unusable which will cause detriment to any part of the Microsoft solution, where this has been provided by the Third Party Partner. |
| **Cryptography** | Mathematical method for securing information from unauthorized access. |
| **Data Classification** | Is a method for assigning a measurable value to data to enable the assignment of appropriate security requirements and restrictions. |
| **Hosting Facility or Hosting Service** | Any physical location or environment not directly owned or leased by Microsoft Corporation, or one of its wholly owned subsidiaries, that is used for hosting of MSN or Windows Live content, web applications, data, company brand, or advertising. |
| **Initial Response** | First contact provided after the Partner has submitted a service request. This response may be in the form of an email message, phone call, and will contain the service request number for tracking purposes. |
| **PII** | **P**ersonally **I**dentifiable **I**nformation is sensitive data that if obtained by unauthorized parties could damage an individual or company. There are varying degrees of PII data. For example, customer name and address is considered to be medium value data that if exposed may impact an individual privacy expectations. If a customer’s credit card information were to be exposed it could significantly impact a customer’s financial status. High value customer information is typically referred to **HSPII** or **H**ighly **S**ensitive **P**ersonally **I**dentifiable **I**nformation. |
| **Security Compromise** | An event that has exposed customer information or confidential data to unauthorized persons has an adverse financial impact, legal standing and/or company reputation. |
| **Security Incident** | Any anomalous activity on a system that affects, or could affect, the confidentiality, integrity, or availability of data or resources. |
| **Service Availability Incident** | An unplanned event that interrupts the normal delivery or service. |
| **Service Border or Perimeter** | Farthest network egress point to the public Internet that is entirely under the direct control of the Microsoft Operations department. |
| **Third Party Partner** | Vendor which provides services pertaining to delivery of content, hosting or application development described in this exhibit. |
| **Site Cloaking** | Method in which a site is made unavailable to the public. Cloaking is used as a last resort as a response to a security incident or significant weaknesses in the site. |
| **Vulnerability** | A weakness which allows an attacker to compromise the integrity of a site, access customer information or otherwise deface the site |