****

**Microsoft Dynamics AX Implementation**

**Application Security Strategy**

**Prepared by**

**(Enter Name Here)**

Contributors

**Revision and Signoff Sheet**

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change reference |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Client Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

Table of Contents

[Revision and Signoff Sheet 2](#_Toc234136772)

[Change Record 2](#_Toc234136773)

[Table of Contents 3](#_Toc234136774)

[1 Summary 5](#_Toc234136775)

[2 Overview 5](#_Toc234136776)

[2.1 Business Objectives 5](#_Toc234136777)

[2.2 Functional Objectives 5](#_Toc234136778)

[2.3 In Scope 5](#_Toc234136779)

[2.4 Out of Scope 6](#_Toc234136780)

[2.5 Assumptions 6](#_Toc234136781)

[2.6 Constraints 7](#_Toc234136782)

[3 Requirements 8](#_Toc234136783)

[3.1 Expense Management Functional Security requirements 8](#_Toc234136784)

[3.2 System Control Requirements 8](#_Toc234136785)

[4 Dynamics AX Security Overview 10](#_Toc234136786)

[4.1 User Accounts 10](#_Toc234136787)

[4.1.1 User Account types 10](#_Toc234136788)

[4.1.2 User Account profiles 10](#_Toc234136789)

[4.1.3 User Account maintenance 10](#_Toc234136790)

[4.1.4 User -> Employee relations 10](#_Toc234136791)

[4.2 Application security components 11](#_Toc234136792)

[4.3 Security role example 13](#_Toc234136793)

[5 Security Role Implementation 14](#_Toc234136794)

[5.1 Security Roles and Responsibilities 14](#_Toc234136795)

[5.2 Security Role Definitions 14](#_Toc234136796)

[5.2.1 Expense Management Dynamics AX roles 14](#_Toc234136797)

[5.2.2 Enterprise Portal SharePoint Security configuration 15](#_Toc234136798)

[6 Security Administration and application support 16](#_Toc234136799)

[6.1 Security Administrator 16](#_Toc234136800)

[6.2 Dynamics AX Systems Application Support 17](#_Toc234136801)

[6.3 User Access Process 17](#_Toc234136802)

[6.3.1 User role assignment overview 18](#_Toc234136803)

[7 Development Environment Security 19](#_Toc234136804)

[7.1 Overview 19](#_Toc234136805)

[7.2 Environments 19](#_Toc234136806)

[7.3 Tools 19](#_Toc234136807)

[7.4 Production Changes 19](#_Toc234136808)

[7.5 Guidelines 19](#_Toc234136809)

[8 Data Classification 21](#_Toc234136810)

[8.1 Data Classification Policy 21](#_Toc234136811)

[8.2 Personal information stored in Dynamics AX 21](#_Toc234136812)

[9 Password Controls and administration 22](#_Toc234136813)

[9.1 Password Policies 22](#_Toc234136814)

[9.2 Screen Lock/Time Out 22](#_Toc234136815)

[9.3 Time/Day Sign On Restrictions 22](#_Toc234136816)

[10 Security Design and related activities 23](#_Toc234136817)

[10.1 Activities by SureStep phase 23](#_Toc234136818)

[10.2 Other project activities 23](#_Toc234136819)

[10.2.1 Detailed Security configuration 23](#_Toc234136820)

[10.2.2 Integration Testing 23](#_Toc234136821)

[10.2.3 User Acceptance Testing 23](#_Toc234136822)

[10.2.4 Issue Resolution 23](#_Toc234136823)

[10.2.5 Change Control 23](#_Toc234136824)

[10.2.6 QA process 23](#_Toc234136825)

[11 Appendix 24](#_Toc234136826)

[11.1 Definitions 24](#_Toc234136827)

[11.1.1 High Business Impact (HBI) 24](#_Toc234136828)

[11.1.2 Moderate Business Impact (MBI) 24](#_Toc234136829)

[11.1.3 Low Business Impact (LBI) 24](#_Toc234136830)

1. Summary

The purpose of this document is to define an application security strategy for the One Finance Expense Management implementation of Dynamics AX 6.0. It will document the functional and technical requirements for security along with the associated security practices and guidelines.

1. Overview
   1. Business Objectives

The business objectives considered in the security approach are the following:

* Integrity of data
* Confidentiality of data
* Availability of data
* Access is granted on a ‘need to do’ basis
  1. Functional Objectives

The functional objectives for this document are the following:

* Ensure that the security features of Dynamics AX enable authorized roles proper access while preventing unauthorized access.
* Specify the security configurations that are required to enable the proper security controls.
* Provide an explanation of the user roles and responsibilities for the Dynamics AX implementation.
* All roles should be configured with the principle of ‘Least Privilege’. Start with the narrowest permissions needed for the role being defined. Start with no privilege and add the required tasks to the role as needed to perform the job function.
* Understand the security capabilities delivered in Dynamics AX 6.0.
  1. In Scope

The Dynamics AX application environment for Microsoft will consist of several layers of security.

Security considerations will need to be taken into account for each layer when designing the overall security model. The layers are shown below:



* **Active Directory security** - used to assign network login ID’s and passwords, restrict Sign On times for users at the network level, and grant file access to the network.
* **Dynamics AX application security** - used to control who can access the Dynamics AX application, what functions they can perform, and what business data they may view, manipulate, or add.
* **License codes** – Enable access at the company level to the areas purchased.
* **Configuration keys** – Enable or disable specific features within the application at the company level.
* **User Roles** – Used to group sets of tasks together to perform specific job functions. A user may have one or more user roles attached to their user profile.
* **Operating system security** - used to control authentication to the O/S, determine what network services are available, and define what files/directories a user can access.
* **Database security** - used to control authentication to the SQL Server database, determines which tables or views users can access determine which commands they can use to manipulate data.
* **Reporting security** –
* **SharePoint** – used to control access to the Enterprise Portal. It operates in conjunction with Dynamics AX application security.
  1. Out of Scope

Security around the following items will not be considered in this document.

* Operating system
* Database
* Network
* Hardware
* Interfaces
* Data conversion
* Business continuity planning
* Disaster recovery
* Source Control
* Server
  1. Assumptions

The performance and completion of this strategy document are predicated on the following assumptions:

* Password management will not be required in Dynamics AX due to integration with Active Directory. Corporate password policies will be enforced and maintained through Active Directory authentication.
* Any related non-Dynamics AX application security will interface effectively with the Dynamics AX System.
* This document will need to be updated after AX 6.0 M3 is released.
* At the highest level of authorization, access to Dynamics AX will be controlled based on whether the user has a valid enabled Active Directory account. The AX user account will be enabled/disabled based on the status of the Active Directory account. The process for enabling/disabling the Active Directory account will follow the existing Microsoft process.
* Code review of AX standard product is out of scope since it has already received the SWI exception.
* It is assumed that the Server Side Trimming vulnerability has been mitigated through one or all of the following:
  + AX TPF for all HBI data
  + Configuration (and no additional customization)
  1. Constraints

The performance and completion of this strategy are predicated on the following constraints:

* Microsoft Infrastructure (Operating System, Network, and database) will develop their own security strategy
* Delivery of the required security functionality for AX 6.0

1. Requirements

A number of requirements have been identified that will need to be taken into consideration in the overall security design in order to meet Microsoft corporate and business policies.

* 1. Expense Management Functional Security requirements
* Comprehensive procedures must exist for adding, removing, or modifying employee access to the Dynamics AX system. These procedures must also encompass the granting and removal of access to the Dynamics AX system for contract and temporary employees.
* All security requests not processed automatically must be approved by designated managers and approvers for additions, changes, and deletions. These individuals should be independent assessors of whether requested security is appropriate and not members of Security Administration personnel.
* Access to Dynamics AX forms must be limited to the appropriate personnel. A user’s requirement for form access must be directly related to the user’s job function.
* Access to Dynamics AX forms must be adequately separated to provide segregation of duties.
* The System Administrator role should be the only role with add, update, display and delete access to Administrative functions such as security settings, user account management, policies, and batch jobs.
* Access to the System Administrator role should be highly restricted. To maintain segregation of duties the functions in the System Administrator role should not be included in any other functional role.
* The ability to run Dynamics AX reports, batches and modify workflows must be limited to specifically defined roles.
* A combination of roles can be assigned to a specific user profile to determine a user’s access to Dynamics AX.
* Procedures for requesting, approving, and amending user profiles or configuration information must be defined and implemented. Additions and changes to user profiles or access configurations are made on the basis of proper approval.
  1. System Control Requirements
* Access to configuration settings are limited to a select number of authorized individuals.
* Changes to configuration settings are properly authorized.
* There will be a change control process in place to analyze the impact of any configuration changes prior to implementation.
* Changes to configuration settings are tested in a test environment, and migrated to Production using the approved migration process.
* Access to Dynamics AX system processing functions and data is adequately segregated and restricted to authorized individuals.
* Dynamics AX data entry and processing functions are reviewed and approved by authorized individuals.
* Dynamics AX application access requirements adhere to the Microsoft corporate security standards.
* Critical Dynamics AX reference and standing data tables are audited to provide an audit trail of changes.
* Dynamics AX transactions processed through the system are complete and accurate.
* Private and confidential Dynamics AX data has been classified, and the appropriate security measures have been implemented to ensure confidentiality of the data.
* There is a clear delineation of functional and technical users of the Dynamics AX system.
* Application security will be applied consistently to all delivered and custom developed forms and reports.

1. Dynamics AX Security Overview

The Dynamics AX environment has a number of security features that will be utilized to control access to the system. An overview of the security features are discussed below.

* 1. User Accounts

Each person who accesses Dynamics AX needs to be set up as a user. In order to create a user account in Dynamics AX the user account must already exist in the Active Directory of the domain of the Dynamics AX installation. Once the user account is set up in AX and given the appropriate permissions the user will have access to the Dynamics AX application through their authenticated network logon without needing to sign into the application directly.

* + 1. User Account types

There are two types of Active Directory user accounts that are applicable for the Dynamics AX implementation:

* **User** – Establishes the identity of a person. Governs network access, Internet and intranet access. Most staff at Microsoft receive a user account.
* **Service** – Runs services, batch jobs and scripts. This would not be assigned to a specific person.
  + 1. User Account profiles

The user account holds data specific to a particular user. Some of these key values are the following:

* Email address
* Startup company account
* Language
* Automatic shutdown
* Notification Preferences
* Assigned roles
  + 1. User Account maintenance

A process will be developed to synchronize the Microsoft Active directory accounts with the Dynamics AX user accounts. This process is outside the scope of this document and will be covered by the master data interface design.

* + 1. User -> Employee relations

Once a user account is set up in Dynamics AX it needs to be linked to a specific employee record. This creates a link between the users network credentials and the employee specific data held in the Dynamics AX HR module.

* 1. Application security components

Once a user account has been established in Dynamics AX the user account can be assigned a role or roles to perform their job function. Each role is composed of task(s) that define specific functional capabilities in the system.



* **Role** - Roles are assigned to users. A role is comprised of a set of tasks that enable a person holding that role to perform specific functions. An example of a role is “Accounts Receivable Clerk”. Dynamics AX will ship with ~80-100 out of the box roles. These roles can be used as is or copied and modified as needed to meet the business requirements. Administrators can also create additional roles as needed.
* **Role Hierarchy** – Roles can also be part of a role hierarchy. The role hierarchy permits defining a role that is comprised of another role or roles. For example an there may be an employee role and a manager role. All managers are employees so instead of defining all employee functions under the manager role again you can create a composite role that includes both the manager and employee roles.
* **Tasks** – In Dynamics AX are a group of permissions that provide access to perform a specific function in the system. One example of a task would be “View Employee Details”. This task would contain the permissions to allow the user access to the form, fields, table and menu items required to view employee details. Dynamics AX will ship with ~10,000 predefined tasks that can be added to roles. These tasks can be used as is or can be modified as needed. Administrators can also create new tasks as needed.
* **Form security** – Restricts access to a form
* **Menu security** – Restricts access to table and /or column access by granting or revoking menu access
* **Row level** – Restricts access to specific records by the use of filters that are applied at the system level.
* **Field level** – Information on a form can be subjectively restricted based on criteria written expressly for that form.
* **Security policies** -
* **Report security** – Controls which users can access reports through menus

**Permission levels**

Each form, menu, field, and table can be restricted by the permission level set for that object. The available levels are described in the following table:

| **Action** | **Description** |
| --- | --- |
| No Access | Completely restricts access to that item and any sub-items it controls. The Open command is disabled. Also, the node is not displayed in the Application Object Tree (AOT). |
| View | Grants access to view the item. The Save, Compile, Lock and Unlock commands are disabled. |
| Edit | Grants access to view and edit the item. The **New**, **Duplicate** and **Rename** commands are disabled. |
| Create | Grants access to view, edit, and create new items. The Delete command is disabled. |
| Full control | Gives full control. No commands are disabled |

* 1. Security role example

The following is an example of how roles and tasks are related and how roles can be assigned to a specific user to accomplish their job functions.



1. Security Role Implementation
   1. Security Roles and Responsibilities

Roles will be defined based on functional requirements of the types of users and their need for access to the Dynamics AX system. These roles in turn lead to the development of specific user profiles that contain the required access to perform duties within Dynamics AX.

The approach to defining the security ‘Roles’ is based on 3 main principles:

* Prevent errors or irregularities occurring within Dynamics AX Systems processing functions by designing roles that ensure the segregation of incompatible duties, reporting access, and system configurations that have security consequences.
* The security roles address access at the menu and function levels
* Security ‘Roles’ should be aligned, as far as possible, with the functional ‘Roles’ defined for Microsoft personnel
  1. Security Role Definitions

The following sub-section provides a high level definition of the planned security ‘Roles’ for the implementation of the Dynamics AX Expense module.

* + 1. Expense Management Dynamics AX roles

These roles are intended for use by users whose job functions require them to access the Dynamics AX Expense module.

Note: Where appropriate, end users may belong to one or more of the following security roles:

| Role | Description |
| --- | --- |
| Expense\_User | * Create expense report * Search expense report |
| Approver | * Expense\_User role * Approve expense report * Search expense report for my org |
| Business\_Approver | * Expense\_User role * Approve expense report * Search expense report for my org |
| MCS\_User | * Create expense report * Search expense report |
| Back\_office | * Search expense reports * Post expense reports |
| Administrator (super-user) | * Full system accesst |
| Security\_Administrator | * Maintain user accounts * Maintain permissions * Maintain tasks * Maintain roles |

All Microsoft employees will be assigned the default Expense\_User role upon creation of their user account in Dynamics AX.

* + 1. Enterprise Portal SharePoint Security configuration

Every user who will need to access the Enterprise Portal site will need to be granted access permissions to the appropriate SharePoint site. SharePoint security works in conjunction with Dynamics AX application security to provide access to the required functions in the Enterprise Portal. SharePoint security grants the user access to the SharePoint site but does not give access to any of the specific Dynamics AX menu options or screens. The user must have the appropriate Dynamics AX role assigned to be able to access the application.

1. Security Administration and application support
   1. Security Administrator

The Dynamics AX Systems Security Administrator is responsible for enforcing corporate security standards and procedures as they relate to the Dynamics AX system. The primary responsibilities of the Security Administrator should be to oversee the following:

* Dynamics AX Systems security strategy,
* Setup and maintenance of Dynamics AX Systems security configurations
* Create and maintain Dynamics AX Systems users
* Assign roles to users

Note: Corporate password standards will be enforced through the integration with Active Directory. It will not be necessary for the Security Administrator to maintain corporate password standards.

The Security Administrator should be the primary contact for resolving application security issues as well as troubleshooting Dynamics AX System security problems.

The Dynamics AX Systems Security Administrator should design, build and implement Dynamics AX security, and coordinate efforts to secure the Dynamics AX Systems on an ongoing basis. This role should also be responsible for ensuring that users receive the appropriate access to the system only after properly completed and approved access request forms have been completed for each user.

The individual must possess technical knowledge of Dynamics AX security, and broad knowledge of the Dynamics AX. The Security Administrator must periodically coordinate with network, O/S, and database administrators to ensure that common issues are resolved. The following additional tasks are also to be performed by the Security Administrator:

* Maintain an up-to-date list of valid authorized approvers.
* Monitor and review security access periodically
* Validate that user accounts permissions are revoked when users leave the company and their Active Directory account is disabled.

The following table summarizes the Security Administrator’s job responsibilities:

| Role | Responsibilities |
| --- | --- |
| Security Administrator | * Oversee security strategy * Set up users * Data auditing * Security configurations (user profiles, security roles) * Technical troubleshooting of the Dynamics AX System application security problems * Segregation of duties * Security housekeeping   + Check for inactive/unused User Ids   + Check security parameters |

The following table defines the application access requirements to Dynamics AX that should exist for the security administration:

| Module | Function |
| --- | --- |
| Administration | Common Forms - Users |
|  | Setup - User Profiles (Role Center) |
|  | Setup – Security functions |
|  | Reports -Security Reports |
| AOT | No Access for Security Administrators |

* 1. Dynamics AX Systems Application Support

Post implementation, Dynamics AX Systems Application Support staff must not have update/display access to Dynamics AX forms in either the thick client or the Enterprise Portal without a valid business reason. It is recommended that these users be limited to display only access to Dynamics AX forms and Enterprise portal pages that are not system administration tools.

Post implementation, access to system administration forms should be granted on the basis of a valid business reason to Application Support roles.

* 1. User Access Process

The user access process for the Dynamics AX System application environments must comply with Microsoft’s existing Security Standards.

All users who have an Active Directory account will automatically have a user profile created in Dynamics AX via an automated master data loading process. However no access permissions will be granted by default. The creation of an Active Directory account will follow the existing process and will not be covered in this document.

Once a user account exists in Dynamics AX a role(s) must be assigned to the user profile so that they will be able to access the appropriate forms, menus, reports and enterprise portal pages to perform their job functions. Roles can be assigned to a user through two different methods:

1. The Security Administrator manually assigns a role to a user using the Role Administrator UI interface.
2. The system will assign role(s) to a user after the user / role assignment has been approved by a manager.
   * 1. User role assignment overview



1. Development Environment Security
   1. Overview

Object security can be used to secure individual objects such as forms, records, menus, queries, etc. The development environment will not have object level permissions activated. However developer level access to the Application Object Tree will granted to specific authorized developers in the development environment. No other users will have access to the Application Object Tree. Development access will not be allowed in the production environment or test environments.

* 1. Environments

In order to maintain the integrity of environment objects and processing, a strict change control process must be in place to ensure that only authorized, valid and appropriate changes are made to the production environment. To support the change control process the following environments will be configured:

* Development
* Test
* PPE / UAT
* Production

Changes to Dynamics AX objects are made in the development environment only. The modified objects are then migrated into the test & PPE environments where the objects are tested to ensure they meet user and system requirements. Finally, the tested and approved object is migrated into the production environment.

* 1. Tools

The ability to migrate objects between instances will be tightly controlled. Only authorized users will have access to the tools used to move objects from the development to test environments, and then from test to production. For each instance, access to these tools will only be granted to a user with appropriate job responsibilities.

* 1. Production Changes

To prevent change control from being circumvented through unauthorized direct changes to production objects, update access to the Application Object Tree tool in the production environment will be restricted from all users, including developers. All changes required for production must be migrated through the test environments before being applied to production.

* 1. Guidelines

The following items summarize and supplement the change control issues discussed above. They are guidelines that should be followed in the development of detailed change control procedures.

* Access to Application Object Tree in test and production environments is restricted from all users.
* At a minimum, four types of environments exist: development, test, PPE and production.
* A mechanism is in place for documenting, collecting, reviewing and approving user change requests. This could be in the form of a change control committee that meets periodically to review and approve change requests.
* Records are maintained and filed for all phases of the process, including user requests, developers changes, and test plans/results.
* Application documentation is updated in a timely manner for all changes.
* An authorized user(s) separate from developers is the only person(s) with access to migration tools in the four environments. All migration requests must flow through this person or group. This allows a single point of contact for all object migrations.
* Only migration and testing users have access to the test environment.
* Development should follow best practices as defined in the AX development standards documentation.

1. Data Classification
   1. Data Classification Policy

All data residing in Dynamics AX will need to be classified and should be labeled with one of the three classification designations HBI, MBI, or LBI. High Business Impact (HBI), Moderate Business Impact (MBI), and Low Business Impact (LBI) are the three internal labels Microsoft uses to classify its information assets. These internal Microsoft classifications must be applied to all Microsoft business information assets, wherever they reside. Once classified, the information must be protected according to the handling requirements based on its defined classification. Please see appendix for complete definitions of HBI, MBI and LBI data classifications.

The full Microsoft policy for information classification can be found [here](http://itweb/Security/Policy/Pages/InfoClass.aspx%23_toc150145630).

* 1. Personal information stored in Dynamics AX

The HBI data classification also includes Highly Sensitive Personally Identifiable Information (PII) which is also subject to Microsoft’s privacy policy. The list below identifies some but not all tables in which Dynamics AX may store personal information:

* Any table that begins with BANK
* Any table that begins with COMMISSION
* COMPANYINFO
* CONTACT
* CUSTTABLE
* EMPLTABLE, and any other table that starts with EMPL
* ECPCUSTSIGNUP
* Any table that begins with HRM
* SYSCOMPANYUSERINFO
* USERINFO
* VENDTABLE

Information stored in these tables should be subject to the controls as specified in the Microsoft information and handling standard for HBI data.

1. Password Controls and administration

Access to the Dynamics AX instance is controlled through integration with Active Directory. If a user has an Active directory account that is not disabled and that user has been set up in Dynamics AX with a user profile they will have access Dynamics AX based on the permissions and roles they have been granted.

* 1. Password Policies

For reference the current Microsoft IT Active Directory password policies are noted below:

* Passwords MUST be configured to be changed at least once every seventy (70) days.
* User objects that use the same account name across other domains MUST have significantly different passwords.
* The non-expiring password flag MUST NOT be set on any user object.
* User objects with administrator privileges are not enabled to require the use of a smart card MUST have passwords that are at least 15 characters long.
* Passwords MUST be configured so they cannot be changed by the account’s owner more than once in a 24 hour time period.
* Passwords MUST be significantly different from the last 24 passwords used for that User Object.
* Passwords MUST NOT be hard-coded into any process or stored unencrypted.

Link to MSIT security policy:  
[Security Policies](http://itweb/Security/Policy/Pages/IdentityAAA.aspx)

* 1. Screen Lock/Time Out

The time-out property is configured at the user level. The time-out property will be set up so that a user will be disconnected from Dynamics AX if the application has been idle for the specified time of 30 minutes.

* 1. Time/Day Sign On Restrictions

There are no restrictions maintained in Dynamics AX in regards to when a user can sign on to the system. The only restrictions would be inherited from the corporate Active Directory settings if any logon time restrictions have been enabled.

1. Security Design and related activities
   1. Activities by SureStep phase

Listed below are the types of security related activities that can be expected by project phase.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Diagnostic | Analysis | Design | Development | Deployment | Operation |
| * Develop application security plan | * Analyze Security Requirements | * Design security tasks * Design security roles * Identify end-users and roles * Build role/task matrix | * Build security objects * Unit test * Migrate security settings to other environments (test, sandbox, etc.) * Integration testing | * Migrate security settings to production | * Perform regular user maintenance |

* 1. Other project activities
     1. Detailed Security configuration

Will be collected and documented in the Microsoft Dynamics AX System Application Security Design spreadsheet.

* + 1. Integration Testing

Will be performed in accordance with the Integration Testing Strategy as detailed in the overall Master test plan.

* + 1. User Acceptance Testing

Will be performed in accordance with the User Acceptance Testing Strategy as detailed in the overall Testing strategy

* + 1. Issue Resolution

**14**. Issue new User Ids and passwords

Who: AC Finance Systems Security

Any Dynamics AX System application security related issues will be addressed through the ‘Issue Resolution’ process as developed for One Finance project.

* + 1. Change Control

Changes to security resulting from business requirements will follow the ‘Change Control’ process developed for the One Finance project.

* + 1. QA process

Quality assurance of the security approach will be maintained through:

Sign off by appropriate business and project personnel

1. Appendix
   1. Definitions
      1. High Business Impact (HBI)

This classification category MUST be assigned to information asset types where unauthorized disclosure could cause severe or catastrophic material loss to Microsoft, the Information Asset Owner, or relying parties.  These are not actual Microsoft classifications but some illustrative examples of what could be classified as HBI by the Information Asset Owner:

* Authentication/authorization credentials and/or information that can be used to directly or indirectly authenticate or authorize valuable transactions
* Information under strict regulatory handling requirements (e.g., [Directive 95/46/EC](http://en.wikipedia.org/wiki/Directive_95/46/EC_on_the_protection_of_personal_data), [GLBA](http://en.wikipedia.org/wiki/GLBA), [HIPAA](http://en.wikipedia.org/wiki/HIPPA), and [CA SB1386](http://en.wikipedia.org/wiki/SB_1386)) and/or business secrets (e.g., unannounced financials, trade secrets)
* Source code, symbols, binaries, or specifications that could negatively impact Microsoft’s competitive advantage or Intellectual Property rights
  + 1. Moderate Business Impact (MBI)

This classification category MUST be assigned to information asset types where unauthorized disclosure could cause serious material loss to Microsoft, the Information Asset Owner, or relying parties.  These are not actual Microsoft classifications but some illustrative examples of what could be classified as MBI by the Information Asset Owner:

* Unreleased product schedules and network infrastructure configurations and/or designs
* Source code or binaries that, if reverse engineered or cloned, could result in serious material impact to the quality and/or integrity of Microsoft products or brand. (e.g. user interfaces)
  + 1. Low Business Impact (LBI)

This classification category MUST be assigned to information asset types where unauthorized disclosure could result in none to limited material loss to Microsoft, the Information Asset Owner, or relying parties.  These are not actual Microsoft classifications but some illustrative examples of what could be classified as LBI by the Information Asset Owner:

* Companywide announcements and information that all employees, contingent staff, and those under NDA have been approved to read
* Source code shared as part of the [Microsoft's Shared Source Initiatives](http://www.microsoft.com/resources/sharedsource/default.mspx) such as information under the Microsoft Public License (Ms-PL), the Microsoft Reciprocal License (Ms-RL), and the Microsoft Reference License