| ITB # | Title | Revised | Type | Summary/Comment |
|---|---|---|---|---|
| **ACC001** | IT Accessibility Policy | 3/16/2006 | Policy | Applications should be compliant with Section 508 of the Rehabilitation Act Amendments of 1998. Note that these standards (as well as the ITB) are in the process of being revised. |
| **APP035** | Internet Browser Policy | 11/25/2009 | Policy | Sets standard for commonwealth desktop browsers per STD-APP035A. Applications should support these browsers at a minimum. |
| **STD-APP035A** | Internet Browser Product Standards | 11/25/2009 | Standard | Internet Explorer 6,7; Mozilla, Firefox, Opera, Internet Explorer 8 |
| **APP036** | Office Productivity Software Policy | 11/25/2009 | Policy | Sets standard for commonwealth desktop office products per STD-APP036A. Reporting to the commonwealth should follow these standards. |
| **STD-APP036A** | Office Productivity Product Standards | 11/25/2009 | Standard | Microsoft Office 2007 products. Older versions are to be retired |
| **APP037** | Document Viewer and Reader Policy | 11/25/2009 | Policy | Sets standard for commonwealth desktop office viewers per STD-APP037A. Reporting to the commonwealth should follow these standards. |
| **STD-APP036A** | Document Viewer and Reader Product Standards | 11/25/2009 | Standard | Document viewers…Microsoft Office 2007 viewers as well as Adobe Acrobat Reader 8.13 and higher. |
| **INF001** | Database Management Systems | 4/17/2009 | Policy | Vendor should use an appropriate database managements system though not necessarily the commonwealth product standards for this. |
| **INF002** | Metadata Standards | 8/17/2007 | Policy | Vendor should use appropriate metadata standards though not necessarily the commonwealth product standards for this. |
| **INF003** | Data Modeling Standards | 8/2/2005 | Policy | Vendor should use appropriate data modeling standards though not necessarily the commonwealth product standards for this. |
| **INFRM006** | Electronic Documents Management Systems | 9/17/2007 | Policy | Vendor should use an appropriate EDMS for the project and other pertinent documentation though not necessarily the commonwealth product standards for this. |
| **PRV001** | Commonwealth of Pennsylvania Electronic Information Privacy Policy | 1/18/2007 | Policy | Vendor should comply with all pertinent federal and state privacy regulations (HIPAA, etc.) |
| **SEC001** | Enterprise Host Security Software Suite Standards and Policy | 8/26/2008 | Policy | Vendor should protect their systems with anti-virus, host intrusion protection, incident response monitoring and reporting, system and application patch management though not necessarily the commonweath product standards for this. |
| **SEC004** | Enterprise Web Application Firewall | 1/15/2010 | Policy | Vendow should install appropriate web application firewall though not necessarily the commonwealth's product standard for this. |
| **SEC007** | Minimum Standards for User ID's and Passwords | 9/7/2006 | Policy | Vendor should comply with minimum user ID, password, account locking, and time-out standards specified in RFD-SEC007A. |
| **RFD-SEC007A** | Commonwealth of Pennsylvania Detailed Windows Password Policy | 10/16/2009 | Policy | Detailed user ID, password, account locking, and time-out standards specified in RFD-SEC007A. |
| **SEC010** | Virtual Private Networks | 2/24/2010 | Policy | If vendor needs VPN between commonwealth and their systems, these policies should be followed. |
| **SEC011** | Enterprise Policy and software Standards for Agency Firewalls | 1/31/2002 | Policy | Vendow should install appropriate network firewalls though not necessarily the commonwealth's product standard for this. |

| | | | | |
|---|---|---|---|---|
| **SEC019** | Policy and procedures for Protecting Commonwealth Electronic Data | 12/14/2009 | Policy | Definition of "C" classification of data…generally Health Information would be considered "C" data. Data should not be stored on non-approved devices or in non-approved facilties; encryption is required for storage and transmission. |
| **SEC020** | Encryption Standards for Data at Rest | 9/17/2009 | Policy | Vendor should encrypt "C" classication data while at rest. |
| **SEC024** | IT Security Incident Reporting Policy | 9/21/2007 | Policy | Vendor should report security incidents to the commonwealth CISO as well as comply with state and federal data breach notifications regulations. |
| **SEC031** | Encryption Standards for Data in Transit | 9/17/2009 | Policy | Vendor should encrypt "C" classication data while in transit. (SEC019) |
| **SEC034** | Enterprise Firewall Rule Set | 8/26/2008 | Policy | Information only: what firewall ports beyond ports 80 and 443 are required to be opened for the vendor's application. |
| **SYM003** | Off-site Storage for Commonwealth Agencies | 12/19/2006 | Policy | Vendor should provide appropriate offsite storage following practices outlined here for distance, environment, etc. |
| **SYM006** | Desktop and Server Software Patching Policy | 11/25/2009 | Policy | Vendor should apply system and application patches per the schedule contained in this ITB. |