

Số: **39** /2017/TT-BTTTT

Hà Nội, ngày **15** tháng **12** năm 2017

|                                 |                       |
|---------------------------------|-----------------------|
| CÔNG THÔNG TIN ĐẾN TỬ CHÍNH PHỦ |                       |
| ĐẾN                             | Giới: <b>S</b>        |
|                                 | Ngày: <b>20/12/17</b> |

## **THÔNG TƯ**

### **Ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước**

*Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;*

*Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;*

*Căn cứ Nghị định số 102/2009/NĐ-CP ngày 06 tháng 11 năm 2009 của Chính phủ về quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;*

*Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;*

*Theo đề nghị của Vụ trưởng Vụ Khoa học và Công nghệ,*

*Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.*

**Điều 1.** Ban hành kèm theo Thông tư này Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước (sau đây gọi là Danh mục).

**Điều 2.** Danh mục này bao gồm các tiêu chuẩn bắt buộc áp dụng hoặc khuyến nghị áp dụng cho hệ thống thông tin của cơ quan nhà nước để bảo đảm kết nối thông suốt, đồng bộ và khả năng chia sẻ, trao đổi thông tin an toàn, thuận tiện giữa các cơ quan nhà nước và giữa cơ quan nhà nước với tổ chức, cá nhân.

Danh mục này cũng được áp dụng để làm căn cứ trong hoạt động đầu tư ứng dụng công nghệ thông tin và thuê dịch vụ công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

**Điều 3.** Trong thời hạn 01 năm kể từ ngày Thông tư này có hiệu lực, hệ thống thông tin của cơ quan nhà nước đang hoạt động cần được rà soát và có phương án, lộ trình chuyển đổi, nâng cấp phù hợp với quy định tại Thông tư này.

**Điều 4.** Vụ Khoa học và Công nghệ có trách nhiệm chủ trì, phối hợp với các đơn vị liên quan định kỳ rà soát, cập nhật Danh mục quy định tại Thông tư này.

Cục Tin học hóa có trách nhiệm hướng dẫn việc áp dụng các tiêu chuẩn kỹ thuật thuộc Danh mục quy định tại Thông tư này.

**Điều 5.** Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2018 và thay thế Thông tư số 22/2013/TT-BTTTT ngày 23 tháng 12 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

**Điều 6.** Chánh Văn phòng, Vụ trưởng Vụ Khoa học và Công nghệ, Cục trưởng Cục Tin học hóa, Thủ trưởng các cơ quan, đơn vị thuộc Bộ, Giám đốc Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương, các tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này. /.

**Nơi nhận:**

- Thủ tướng Chính phủ và các PTTg CP (để b/c);
- Văn phòng TW và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Văn phòng Quốc hội;
- Ban Chỉ đạo Quốc gia về CNTT;
- Ban Chỉ đạo CNTT của cơ quan Đảng;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Tòa án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc CP;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc TW;
- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Công báo;
- Cổng thông tin điện tử Chính phủ;
- Bộ TT&TT:
  - + Bộ trưởng và các Thứ trưởng;
  - + Các cơ quan, đơn vị thuộc Bộ;
  - + Cổng thông tin điện tử Bộ;
- Lưu: VT, KHCN (255b).

**BỘ TRƯỞNG**



**Trương Minh Tuấn**

**DANH MỤC TIÊU CHUẨN KỸ THUẬT  
VỀ ỨNG DỤNG CÔNG NGHỆ THÔNG TIN TRONG CƠ QUAN NHÀ NƯỚC**

(Ban hành kèm theo Thông tư số 39.../2017/TT-BTTTT ngày 15 tháng 12 năm 2017  
của Bộ trưởng Bộ Thông tin và Truyền thông)

| Số TT    | Loại tiêu chuẩn                       | Ký hiệu tiêu chuẩn | Tên đầy đủ của tiêu chuẩn   | Quy định áp dụng                                   |
|----------|---------------------------------------|--------------------|---|--|
| <b>1</b> | <b>Tiêu chuẩn về kết nối</b>          |                    |   |  |
| 1.1      | Truyền siêu văn bản                   | HTTP v1.1          | Hypertext Transfer Protocol version 1.1                             | Bắt buộc áp dụng                                   |
|          |                                       | HTTP v2.0          | Hypertext Transfer Protocol version 2.0                             | Khuyến nghị áp dụng                                |
| 1.2      | Truyền tệp tin                        | FTP                | File Transfer Protocol  | Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn        |
|          |                                       | HTTP v1.1          | Hypertext Transfer Protocol version 1.1                             |  |
|          |                                       | HTTP v2.0          | Hypertext Transfer Protocol version 2.0                             | Khuyến nghị áp dụng                                |
|          |                                       | WebDAV             | Web-based Distributed Authoring and Versioning                      | Khuyến nghị áp dụng                                |
| 1.3      | Truyền, phát luồng âm thanh/ hình ảnh | RTSP               | Real-time Streaming Protocol  | Khuyến nghị áp dụng                                |
|          |                                       | RTP                | Real-time Transport Protocol  | Khuyến nghị áp dụng                                |
|          |                                       | RTCP               | Real-time Control Protocol  | Khuyến nghị áp dụng                                |
| 1.4      | Truy cập và chia sẻ dữ liệu           | OData v4           | Open Data Protocol version 4.0                                      | Khuyến nghị áp dụng                                |
| 1.5      | Truyền thư điện tử                    | SMTP/MIME          | Simple Mail Transfer Protocol/Multipurpose Internet Mail Extensions | Bắt buộc áp dụng                                   |
| 1.6      | Cung cấp dịch vụ truy cập             | POP3               | Post Office Protocol version 3                                      | Bắt buộc áp dụng cả hai tiêu chuẩn đối với máy chủ |
|          | hộp thư điện tử                       | IMAP 4rev1         | Internet Message Access Protocol version 4 revision 1               |  |

|      |  |                     |   |   |
|------|--|---------------------|---|---|
| 1.7  | Truy cập thư mục                         | LDAP v3             | Lightweight Directory Access Protocol version 3                           | Bắt buộc áp dụng  |
| 1.8  | Dịch vụ tên miền                         | DNS                 | Domain Name System  | Bắt buộc áp dụng  |
| 1.9  | Giao vận mạng có kết nối                 | TCP                 | Transmission Control Protocol   | Bắt buộc áp dụng  |
| 1.10 | Giao vận mạng không kết nối              | UDP                 | User Datagram Protocol  | Bắt buộc áp dụng  |
| 1.11 | Liên mạng LAN/WAN                        | IPv4                | Internet Protocol version 4   | Bắt buộc áp dụng  |
|      |  | IPv6                | Internet Protocol version 6   | Bắt buộc áp dụng đối với các thiết bị có kết nối Internet |
| 1.12 | Mạng cục bộ không dây                    | IEEE 802.11g        | Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11g | Bắt buộc áp dụng  |
|      |  | IEEE 802.11n        | Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11n | Khuyến nghị áp dụng                                       |
| 1.13 | Truy cập Internet với thiết bị không dây | WAP v2.0            | Wireless Application Protocol version 2.0                                 | Bắt buộc áp dụng  |
| 1.14 | Dịch vụ Web dạng SOAP                    | SOAP v1.2           | Simple Object Access Protocol version 1.2                                 | Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn           |
|      |  | WSDL V2.0           | Web Services Description Language version 2.0                             |   |
|      |  | UDDI v3             | Universal Description, Discovery and Integration version 3                |   |
| 1.15 | Dịch vụ Web dạng RESTful                 | RESTful web service | Representational state transfer   | Khuyến nghị áp dụng                                       |
| 1.16 | Dịch vụ đặc tả Web                       | WS BPEL v2.0        | Web Services Business Process Execution Language Version 2.0              | Khuyến nghị áp dụng                                       |

|      |                           |  |  |   |
|------|---------------------------|--|--|---|
|      |                           | WS-I Simple SOAP Binding Profile Version 1.0     | Simple SOAP Binding Profile Version 1.0      | Khuyến nghị áp dụng                       |
|      |                           | WS-Federation v1.2                               | Web Services Federation Language Version 1.2 | Khuyến nghị áp dụng                       |
|      |                           | WS-Addressing v1.0                               | Web Services Addressing 1.0                  | Khuyến nghị áp dụng                       |
|      |                           | WS-Coordination Version 1.2                      | Web Services Coordination Version 1.2        | Khuyến nghị áp dụng                       |
|      |                           | WS-Policy v1.2                                   | Web Services Coordination Version 1.2        | Khuyến nghị áp dụng                       |
|      |                           | OASIS Web Services Business Activity Version 1.2 | Web Services Business Activity Version 1.2   | Khuyến nghị áp dụng                       |
|      |                           | WS-Discovery Version 1.1                         | Web Services Dynamic Discovery Version 1.1   | Khuyến nghị áp dụng                       |
|      |                           | WS-MetadataExchange                              | Web Services Metadata Exchange               | Khuyến nghị áp dụng                       |
| 1.17 | Dịch vụ đồng bộ thời gian | NTPv3  | Network Time Protocol version 3              | Bắt buộc áp dụng một trong hai tiêu chuẩn |
|      |                           | NTPv4  | Network Time Protocol version 4              |   |

| <b>2 Tiêu chuẩn về tích hợp dữ liệu</b> |  |                                    |   |   |
|---|--|------------------------------------|---|---|
| 2.1                                     | Ngôn ngữ định dạng văn bản                       | XML v1.0 (5 <sup>th</sup> Edition) | Extensible Markup Language version 1.0 (5 <sup>th</sup> Edition)  | Bắt buộc áp dụng một trong hai tiêu chuẩn |
|   |  | XML v1.1 (2 <sup>nd</sup> Edition) | Extensible Markup Language version 1.1                            |   |
| 2.2                                     | Ngôn ngữ định dạng văn bản cho giao dịch điện tử | ISO/TS 15000:2014                  | Electronic Business Extensible Markup Language (ebXML)            | Bắt buộc áp dụng                          |
| 2.3                                     | Định nghĩa các lược đồ trong tài liệu XML        | XML Schema V1.1                    | XML Schema version 1.1  | Bắt buộc áp dụng                          |
| 2.4                                     | Biến đổi dữ liệu                                 | XSL                                | Extensible Stylesheet Language                                    | Bắt buộc áp dụng phiên bản mới nhất.      |
| 2.5                                     | Mô hình hóa đối tượng                            | UML v2.5                           | Unified Modelling Language version 2.5                            | Khuyến nghị áp dụng                       |
| 2.6                                     | Mô tả tài nguyên dữ liệu                         | RDF                                | Resource Description Framework                                    | Khuyến nghị áp dụng                       |
|   |  | OWL                                | Web Ontology Language   | Khuyến nghị áp dụng                       |
| 2.7                                     | Trình diễn bộ ký tự                              | UTF-8                              | 8-bit Universal Character Set (UCS)/Unicode Transformation Format | Bắt buộc áp dụng                          |
| 2.8                                     | Khuôn thức trao đổi thông tin địa lý             | GML v3.3                           | Geography Markup Language version 3.3                             | Bắt buộc áp dụng                          |
| 2.9                                     | Truy cập và cập nhật các thông tin địa lý        | WMS v1.3.0                         | OpenGIS Web Map Service version 1.3.0                             | Bắt buộc áp dụng                          |
|   |  | WFS v1.1.0                         | Web Feature Service version 1.1.0                                 | Bắt buộc áp dụng                          |
| 2.10                                    | Trao đổi dữ liệu đặc tả tài liệu XML             | XMI v2.4.2                         | XML Metadata Interchange version 2.4.2                            | Khuyến nghị áp dụng                       |

|          |   |                    |   |  |
|----------|---|--------------------|---|--|
| 2.11     | Sổ đăng ký siêu dữ liệu (MDR)                                       | ISO/IEC 11179:2015 | Sổ đăng ký siêu dữ liệu (Metadata registries - MDR) | Khuyến nghị áp dụng                      |
| 2.12     | Bộ phân tử siêu dữ liệu Dublin Core                                 | ISO 15836-1:2017   | Bộ phân tử siêu dữ liệu Dublin Core                 | Khuyến nghị áp dụng(*)                   |
| 2.13     | Định dạng trao đổi dữ liệu mô tả đối tượng dạng kịch bản JavaScript | JSON RFC 7159      | JavaScript Object Notation                          | Khuyến nghị áp dụng                      |
| 2.14     | Ngôn ngữ mô hình quy trình nghiệp vụ                                | BPMN 2.0           | Business Process Model and Notation version 2.0     | Khuyến nghị áp dụng                      |
| <b>3</b> | <b>Tiêu chuẩn về truy cập thông tin</b>                             |                    |   |  |
| 3.1      | Chuẩn nội dung Web  | HTML v4.01         | Hypertext Markup Language version 4.01              | Bắt buộc áp dụng                         |
|          |   | WCAG 2.0           | W3C Web Content Accessibility Guidelines (WCAG) 2.0 | Khuyến nghị áp dụng                      |
|          |   | HTML 5             | Hypertext Markup Language version 5                 | Khuyến nghị áp dụng                      |
| 3.2      | Chuẩn nội dung Web mở rộng  | XHTML v1.1         | Extensible Hypertext Markup Language version 1.1    | Bắt buộc áp dụng                         |
| 3.3      | Giao diện người dùng  | CSS2               | Cascading Style Sheets Language Level 2             | Bắt buộc áp dụng một trong ba tiêu chuẩn |
|          |   | CSS3               | Cascading Style Sheets Language Level 3             |  |
|          |   | XSL                | Extensible Stylesheet Language version              |  |

(\*) Đối với các đối tượng thuộc phạm vi điều chỉnh của Thông tư số 24/2011/TT-BTTTT thì vẫn áp dụng quy định của Thông tư số 24/2011/TT-BTTTT.

|     |            |                               |   |   |
|-----|------------|-------------------------------|---|---|
| 3.4 | Văn bản    | (.txt)                        | Định dạng Plain Text (.txt):<br>Dành cho các tài liệu cơ bản không có cấu trúc  | Bắt buộc áp dụng                                |
|     |            | (.rtf) v1.8, v1.9.1           | Định dạng Rich Text (.rtf) phiên bản 1.8, 1.9.1: Dành cho các tài liệu có thể trao đổi giữa các nền khác nhau           | Bắt buộc áp dụng                                |
|     |            | (.docx)                       | Định dạng văn bản Word mở rộng của Microsoft (.docx)  | Khuyến nghị áp dụng                             |
|     |            | (.pdf) v1.4, v1.5, v1.6, v1.7 | Định dạng Portable Document (.pdf) phiên bản 1.4, 1.5, 1.6, 1.7: Dành cho các tài liệu chỉ đọc                          | Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn |
|     |            | (.doc)                        | Định dạng văn bản Word của Microsoft (.doc)   |   |
|     |            | (.odt) v1.2                   | Định dạng Open Document Text (.odt) phiên bản 1.2   |   |
| 3.5 | Bảng tính  | (.csv)                        | Định dạng Comma eparated Variable/Delimited (.csv):<br>Dành cho các bảng tính cần trao đổi giữa các ứng dụng khác nhau. | Bắt buộc áp dụng                                |
|     |            | (.xlsx)                       | Định dạng bảng tính Excel mở rộng của Microsoft (.xlsx)   | Khuyến nghị áp dụng                             |
|     |            | (.xls)                        | Định dạng bảng tính Excel của Microsoft (.xls)  | Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn     |
|     |            | (.ods) v1.2                   | Định dạng Open Document Spreadsheets (.ods) phiên bản 1.2   |   |
| 3.6 | Trình diễn | (.htm)                        | Định dạng Hypertext Document (.htm): cho các trình bày được trao đổi thông qua các loại trình duyệt khác nhau           | Bắt buộc áp dụng                                |
|     |            | (.pptx)                       | Định dạng PowerPoint mở rộng của Microsoft (.pptx)  | Khuyến nghị áp dụng                             |
|     |            | (.pdf)                        | Định dạng Portable Document (.pdf): cho các trình bày lưu dưới dạng chỉ đọc   | Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn |
|     |            | (.ppt)                        | Định dạng PowerPoint (.ppt) của Microsoft   |   |



|      |                           |                              |   |  |
|------|---------------------------|------------------------------|---|--|
|      |                           | (.odp) v1.2                  | Định dạng Open Document Presentation (.odp) phiên bản 1.2               |  |
| 3.7  | Ảnh đồ họa                | JPEG                         | Joint Photographic Expert Group (.jpg)                                  | Bắt buộc áp dụng một, hai, ba hoặc cả bốn tiêu chuẩn |
|      |                           | GIF v89a                     | Graphic Interchange (.gif) version 89a                                  |  |
|      |                           | TIFF                         | Tag Image File (.tif)   |  |
|      |                           | PNG                          | Portable Network Graphics (.png)  |  |
| 3.8  | Ảnh gắn với toạ độ địa lý | GEO TIFF                     | Tagged Image File Format for GIS applications                           | Bắt buộc áp dụng                                     |
| 3.9  | Phim ảnh, âm thanh        | MPEG-1                       | Moving Picture Experts Group-1  | Khuyến nghị áp dụng                                  |
|      |                           | MPEG-2                       | Moving Picture Experts Group-2  | Khuyến nghị áp dụng                                  |
|      |                           | MPEG-4                       | Moving Picture Experts Group-4  | Khuyến nghị áp dụng                                  |
|      |                           | MP3                          | MPEG-1 Audio Layer 3  | Khuyến nghị áp dụng                                  |
|      |                           | AAC                          | Advanced Audio Coding   | Khuyến nghị áp dụng                                  |
| 3.10 | Luồng phim ảnh, âm thanh  | (.asf), (.wma), (.wmv)       | Các định dạng của Microsoft Windows Media Player (.asf), (.wma), (.wmv) | Khuyến nghị áp dụng                                  |
|      |                           | (.ra), (.rm), (.ram), (.rmm) | Các định dạng Real Audio/Real Video (.ra), (.rm), (.ram), (.rmm)        | Khuyến nghị áp dụng                                  |
|      |                           | (.avi), (.mov), (.qt)        | Các định dạng Apple Quicktime (.avi), (.mov), (.qt)                     | Khuyến nghị áp dụng                                  |
| 3.11 | Hoạt họa                  | GIF v89a                     | Graphic Interchange (.gif) version 89a                                  | Khuyến nghị áp dụng                                  |
|      |                           | (.swf)                       | Định dạng Macromedia Flash (.swf)                                       | Khuyến nghị áp dụng                                  |
|      |                           | (.swf)                       | Định dạng Macromedia Shockwave (.swf)                                   | Khuyến nghị áp dụng                                  |
|      |                           | (.avi), (.qt), (.mov)        | Các định dạng Apple Quicktime (.avi), (.qt), (.mov)                     | Khuyến nghị áp dụng                                  |

|          |  |                |  |   |
|----------|--|----------------|--|---|
| 3.12     | Chuẩn nội dung cho thiết bị di động                | WML v2.0       | Wireless Markup Language version 2.0                                 | Bắt buộc áp dụng                            |
| 3.13     | Bộ ký tự và mã hóa                                 | ASCII          | American Standard Code for Information Interchange                   | Bắt buộc áp dụng                            |
| 3.14     | Bộ ký tự và mã hóa cho tiếng Việt                  | TCVN 6909:2001 | TCVN 6909:2001 “Công nghệ thông tin - Bộ mã ký tự tiếng Việt 16-bit” | Bắt buộc áp dụng                            |
| 3.15     | Nén dữ liệu  | Zip            | Zip (.zip)   | Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn |
|          |  | .gz v4.3       | GNU Zip (.gz) version 4.3  |   |
| 3.16     | Ngôn ngữ kịch bản phía trình khách                 | ECMA 262       | ECMAScript version 6 (6 <sup>th</sup> Edition)                       | Bắt buộc áp dụng                            |
| 3.17     | Chia sẻ nội dung Web                               | RSS v1.0       | RDF Site Summary version 1.0   | Bắt buộc áp dụng một trong hai tiêu chuẩn   |
|          |  | RSS v2.0       | Really Simple Syndication version 2.0                                |   |
|          |  | ATOM v1.0      | ATOM version 1.0   | Khuyến nghị áp dụng                         |
| 3.18     | Chuẩn kết nối ứng dụng công nghệ thông tin điện tử | JSR 168        | Java Specification Requests 168 (Portlet Specification)              | Bắt buộc áp dụng                            |
|          |  | JSR 286        | Java Specification Requests 286 (Portlet Specification)              | Khuyến nghị áp dụng                         |
|          |  | WSRP v1.0      | Web Services for Remote Portlets version 1.0                         | Bắt buộc áp dụng                            |
|          |  | WSRP v2.0      | Web Services for Remote Portlets version 2.0                         | Khuyến nghị áp dụng                         |
| <b>4</b> | <b>Tiêu chuẩn về an toàn thông tin</b>             |                |  |   |
| 4.1      | An toàn thư điện tử                                | S/MIME v3.2    | Secure Multi-purpose Internet Mail Extensions version 3.2            | Bắt buộc áp dụng                            |
|          |  | OpenPGP        | OpenPGP  | Khuyến nghị áp dụng                         |

|     |                                      |                |  |   |
|-----|--------------------------------------|----------------|--|---|
| 4.2 | An toàn tầng giao vận                | SSH v2.0       | Secure Shell version 2.0                                       | Bắt buộc áp dụng  |
|     |                                      | TLS v1.2       | Transport Layer Security version 1.2                           | Bắt buộc áp dụng  |
| 4.3 | An toàn truyền tệp tin               | HTTPS          | Hypertext Transfer Protocol Secure                             | Bắt buộc áp dụng  |
|     |                                      | FTPS           | File Transfer Protocol Secure                                  | Khuyến nghị áp dụng                                       |
|     |                                      | SFTP           | SSH File Transfer Protocol                                     | Khuyến nghị áp dụng                                       |
| 4.4 | An toàn truyền thư điện tử           | SMTPTS         | Simple Mail Transfer Protocol Secure                           | Bắt buộc áp dụng  |
| 4.5 | An toàn dịch vụ truy cập hộp thư     | POP3S          | Post Office Protocol version 3 Secure                          | Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn               |
|     |                                      | IMAPS          | Internet Message Access Protocol Secure                        |   |
| 4.6 | An toàn dịch vụ DNS                  | DNSSEC         | Domain Name System Security Extensions                         | Khuyến nghị áp dụng                                       |
| 4.7 | An toàn tầng mạng                    | IPsec - IP ESP | Internet Protocol security với IP ESP                          | Bắt buộc áp dụng  |
| 4.8 | An toàn thông tin cho mạng không dây | WPA2           | Wi-fi Protected Access 2                                       | Bắt buộc áp dụng  |
| 4.9 | Giải thuật mã hóa                    | TCVN 7816:2007 | Công nghệ thông tin. Kỹ thuật mật mã thuật toán mã dữ liệu AES | Khuyến nghị áp dụng                                       |
|     |                                      | 3DES           | Triple Data Encryption Standard                                | Khuyến nghị áp dụng                                       |
|     |                                      | PKCS #1 V2.2   | RSA Cryptography Standard - version 2.2                        | Khuyến nghị áp dụng, sử dụng lược đồ RSAES-OAEP để mã hóa |
|     |                                      | ECC            | Elliptic Curve Cryptography                                    | Khuyến nghị áp dụng                                       |

|      |                                     |                                      |   |  |
|------|-------------------------------------|--------------------------------------|---|--|
| 4.10 | Giải thuật chữ ký số                | PKCS #1 V2.2                         | RSA Cryptography Standard - version 2.2   | Bắt buộc áp dụng, sử dụng lược đồ RSASSA-PSS để ký |
|      |                                     | ECDSA                                | Elliptic Curve Digital Signature Algorithm  | Khuyến nghị áp dụng                                |
| 4.11 | Giải thuật băm cho chữ ký số        | SHA-2                                | Secure Hash Algorithms-2  | Khuyến nghị áp dụng                                |
| 4.12 | Giải thuật truyền khóa              | RSA-KEM                              | Rivest-Shamir-Adleman - KEM (Key Encapsulation Mechanism) Key Transport Algorithm | Bắt buộc áp dụng                                   |
|      |                                     | ECDHE                                | Elliptic Curve Diffie Hellman Ephemeral   | Khuyến nghị áp dụng                                |
| 4.13 | Giải pháp xác thực người sử dụng    | SAML v2.0                            | Security Assertion Markup Language version 2.0                                    | Khuyến nghị áp dụng                                |
| 4.14 | An toàn trao đổi bản tin XML        | XML Encryption Syntax and Processing | XML Encryption Syntax and Processing  | Bắt buộc áp dụng                                   |
|      |                                     | XML Signature Syntax and Processing  | XML Signature Syntax and Processing   | Bắt buộc áp dụng                                   |
| 4.15 | Quản lý khóa công khai bản tin XML  | XKMS v2.0                            | XML Key Management Specification version 2.0                                      | Khuyến nghị áp dụng                                |
| 4.16 | Giao thức an toàn thông tin cá nhân | P3P v1.1                             | Platform for Privacy Preferences Project version 1.1                              | Khuyến nghị áp dụng                                |

|  |                               |  |                        |
|--|-------------------------------|--|------------------------|
| Hạ tầng khóa công khai                             |                               |  | Khuyến nghị<br>áp dụng |
| Cú pháp<br>thông điệp<br>mật mã cho<br>ký, mã hóa  | PKCS#7<br>v1.5 (RFC<br>2315)  | Cryptographic message<br>syntax for file-based signing<br>and encrypting version 1.5 |                        |
| Cú pháp<br>thông tin<br>thẻ mật mã                 | PKCS#15<br>v1.1               | Cryptographic token<br>information syntax version<br>1.1                             |                        |
| Cú pháp<br>thông tin<br>khóa riêng                 | PKCS#8<br>V1.2 (RFC<br>5958)  | Private-Key Information<br>Syntax Standard version 1.2                               |                        |
| Giao diện<br>thẻ mật mã                            | PKCS#11<br>v2.20              | Cryptographic token<br>interface standard version<br>2.20                            |                        |
| Cú pháp<br>trao đổi<br>thông tin cá<br>nhân        | PKCS#12<br>v1.1               | Personal Information<br>Exchange Syntax version 1.1                                  |                        |
| Khuôn dạng<br>danh sách<br>chứng thư<br>số thu hồi | RFC 5280                      | Certificate Revocation List<br>Profile   |                        |
| Khuôn dạng<br>chứng thư<br>số                      | RFC 5280                      | Public Key Infrastructure<br>Certificate   |                        |
| Cú pháp<br>yêu cầu<br>chứng thực                   | PKCS#10<br>v1.7 (RFC<br>2986) | Certification Request Syntax<br>Specification version 1.7                            |                        |
| Giao thức<br>trạng thái<br>chứng thư<br>trực tuyến | RFC 6960                      | On-line Certificate status<br>protocol   |                        |
| Giao thức<br>gắn tem<br>thời gian                  | RFC 3161                      | Time stamping protocol   |                        |

|      |  |  |   |                     |
|------|--|--|---|---------------------|
|      | Dịch vụ tem thời gian                          | ISO/IEC 18014-1:2008<br>ISO/IEC 18014-2:2009<br>ISO/IEC 18014-3:2009<br>ISO/IEC 18014-4:2015 | Information technology Security techniques – Time stamping services<br>Part 1: Framework<br>Part 2: Mechanisms producing independent tokens<br>Part 3: Mechanisms producing linked tokens<br>Part 4: Traceability of time sources |                     |
| 4.18 | An toàn cho dịch vụ Web                        | WS-Security v1.1.1   | Web Services Security: SOAP Message Security Version 1.1.1  | Khuyến nghị áp dụng |
| 4.19 | Khuôn dạng dữ liệu trao đổi sự cố an toàn mạng | RFC 7970   | The Incident Object Description Exchange Format version 2 (IODEF)   | Khuyến nghị áp dụng |

10