

Số: **30** /KH-UBND

Hà Nội, ngày **24** tháng 01 năm 2014

## **KẾ HOẠCH**

### **Đảm bảo an toàn thông tin số của thành phố Hà Nội đến năm 2015**

#### **I. CÁC CĂN CỨ PHÁP LÝ XÂY DỰNG KẾ HOẠCH**

- Luật Công nghệ thông tin đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khoá XI, kỳ họp thứ 9 thông qua ngày 29 tháng 6 năm 2006;
- Luật Giao dịch điện tử số 51/2005/QH11 ngày 29 tháng 11 năm 2005 do Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam ban hành;
- Nghị định số 64/2007/NĐ-CP ngày 10 tháng 04 năm 2007 của Chính phủ về việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;
- Quyết định số 1605/QĐ-TTg ngày 27/8/2010 của Thủ tướng Chính phủ về việc phê duyệt Chương trình quốc gia về ứng dụng CNTT trong hoạt động của cơ quan nhà nước giai đoạn 2011-2015;
- Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác;
- Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ về việc phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;
- Chỉ thị số 897/CT-TTg ngày 10/06/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;
- Thông tư số 23/2011/TT-BTTTT ngày 11 tháng 08 năm 2011 của Bộ Thông tin và Truyền thông Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;
- Thông tư số 27/2011/TT-BTTTT ngày 04 tháng 10 năm 2011 của Bộ Thông tin và Truyền thông Quy định về điều phối các hoạt động ứng cứu sự cố mạng internet Việt Nam;
- Công văn số 1750/BTTTT-CNTT ngày 09 tháng 7 năm 2012 của Bộ Thông tin và Truyền thông về việc hướng dẫn xây dựng kế hoạch phát triển và ứng dụng CNTT năm 2013 và giai đoạn 2013-2015;
- Quyết định số 3855/QĐ-UBND ngày 28 tháng 8 năm 2012 của UBND thành phố Hà Nội về việc ban hành chương trình mục tiêu ứng dụng CNTT trong hoạt động của cơ quan nhà nước thành phố Hà Nội giai đoạn 2012-2015.

#### **II. HIỆN TRẠNG ĐẢM BẢO AN TOÀN THÔNG TIN SỐ TRONG HOẠT ĐỘNG CỦA CƠ QUAN NHÀ NƯỚC THÀNH PHỐ HÀ NỘI**

## **1. Tình hình thực hiện và ban hành các cơ chế chính sách về đảm bảo an toàn thông tin số**

Việc đảm bảo an toàn thông tin số trong hoạt động của cơ quan nhà nước thành phố Hà Nội đã được thực hiện từ nhiều năm nay thông qua các văn bản chỉ đạo như Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ, Chỉ thị số 897/CT-TTg ngày 10/06/2011 của Thủ tướng Chính phủ; Thông tư số 23/2011/TT-BTTTT ngày 11/08/2011 của Bộ Thông tin và Truyền thông.

Để đảm bảo việc quản lý an toàn thông tin số, Thành ủy- HĐND-UBND Thành phố đã ban hành nhiều chỉ thị, nghị quyết, quyết định, kế hoạch chỉ đạo có liên quan đến đảm bảo an toàn thông tin số trong hoạt động của các cơ quan nhà nước của thành phố Hà Nội.

## **2. Hạ tầng kỹ thuật công nghệ thông tin**

- Mạng LAN và Internet: 100% các sở, ban, ngành và UBND quận, huyện, thị xã đều đã có mạng nội bộ (LAN) và Internet kết nối tới tất cả các phòng, ban. 100% các xã, phường có kết nối Internet (mỗi xã, phường có từ 1-2 đường truyền). Các phường của các UBND Quận đều đã có kết nối LAN, 5 huyện đã có đầu tư mạng LAN cho tất cả các xã (Phúc Thọ, Quốc Oai, Thạch Thất, Thường Tín, Từ Liêm). Đối với các xã, phường không có mạng LAN, có khoảng 50-70% máy tính kết nối Internet.

- Hệ thống an toàn bảo mật: 22/28 sở, ban, ngành và 20/29 quận, huyện đã có phòng máy chủ riêng; 15/28 sở, ban, ngành và 13/29 quận, huyện đã trang bị thiết bị tường lửa; 4 sở, ngành (Sở Thông tin truyền thông, Thanh tra Thành phố, Văn phòng UBND Thành phố, Cục thuế) và huyện Thanh Trì đã trang bị hệ thống cảnh báo truy nhập trái phép; 21/28 sở, ban, ngành và 19/29 quận, huyện đã sử dụng phần mềm diệt virus (miễn phí và bản quyền) cho các máy trạm và trung bình mỗi đơn vị có khoảng 35% máy trạm được cài đặt; các xã, phường chỉ trang bị phần mềm diệt virus cho một vài máy tính (kế toán, văn thư).

Về cơ bản hạ tầng công nghệ thông tin trong các cơ quan nhà nước đáp ứng được nhu cầu ứng dụng trong nội bộ cơ quan. Các đơn vị đã đưa vào khai thác, sử dụng hạ tầng thiết bị công nghệ thông tin có hiệu quả trong công việc tuy nhiên hầu hết các đơn vị chưa được chú trọng đầu tư các trang thiết bị phục vụ công tác bảo đảm an toàn, bảo mật thông tin mạng như: các hệ thống phòng chống xâm nhập, lưu trữ, back up dữ liệu.

## **3. Ứng dụng**

- Hệ thống thư điện tử công vụ của Thành phố: hoạt động ổn định với số lượng 19.529 hòm thư điện tử @hanoi.gov.vn đã được cấp, trong đó: Cấp 15.427 hòm thư cá nhân cho CBCCVV phục vụ trong công tác chuyên môn (trong đó cấp 9.563/10.383 đạt 92% cho cán bộ công chức và 4.522/10.551 đạt 43% cho viên chức của Thành phố). Cấp 2.665 hòm thư công vụ trong Thành phố (phục vụ đối tượng văn thư, kỹ thuật, tổ chức hành chính các cấp, mục tiêu quản lý, điều hành chung trong Thành phố); Cấp 2.779 hòm thư cá nhân, công vụ hỗ trợ các cơ quan Đảng, tổ chức chính trị, cơ quan khác trong Thành phố.

Hầu hết cán bộ, công chức, viên chức đã sử dụng thư điện tử công vụ trong công việc. Do thói quen, một số cán bộ công chức, viên chức vẫn sử dụng một số hệ thống thư công cộng như Gmail, Yahoo... trong khi trao đổi công việc là một phần nguyên nhân ảnh hưởng đến mức độ an toàn, an ninh thông tin cho Hệ thống Thư điện tử Thành phố.

- Hệ thống quản lý văn bản và hồ sơ công việc đã đưa vào ứng dụng tại 100% các sở, ban, ngành, quận, huyện, thị xã và gần 30% xã, phường, thị trấn và bước đầu hình thành kết nối với Hệ thống Quản lý văn bản và Điều hành của Thành phố để phục vụ giao dịch hành chính điện tử hoàn toàn trên ứng dụng trong công tác quản lý, chỉ đạo, điều hành của Lãnh đạo UBND Thành phố và Lãnh đạo các sở, ban, ngành, UBND các quận, huyện, thị xã trong Thành phố. Tính đến thời điểm hiện tại, 100% văn bản chỉ đạo điều hành của Lãnh đạo UBND Thành phố; 82% văn bản đi/đến của các sở, ban, ngành và 74% của UBND quận, huyện, thị xã được lưu trữ trên phần mềm; 40% sở, ban, ngành và 23% UBND quận, huyện, thị xã đã điều hành tác nghiệp trên phần mềm.

- 96,5% sở, ban, ngành, UBND quận, huyện, thị xã có trang/cổng thông tin điện tử (TTĐT) cung cấp các thông tin về hoạt động của đơn vị và 69 dịch vụ công trực tuyến mức độ 3.

- Các hệ thống thông tin, cơ sở dữ liệu đang tiếp tục được hoàn thiện như: Quản lý hộ tịch, Văn hóa- thể thao - du lịch, Quy hoạch xây dựng, Quy hoạch đô thị, Tài nguyên môi trường, Đăng ký kinh doanh cấp huyện, Dân cư, Quản lý khu đô thị mới,...

- Ngoài ra còn có trên 270 phần mềm nội bộ hỗ trợ tác nghiệp đang ứng dụng tại các cơ quan nhà nước.

#### **4. Nguồn nhân lực bảo đảm an toàn thông tin số**

- Trên 90% cán bộ, công chức, viên chức sử dụng thành thạo máy tính và các phần mềm: soạn thảo văn bản, truy cập internet (firefox, IE,..), thư điện tử, quản lý văn bản, unikey, ... Tuy nhiên kiến thức đảm bảo an toàn thông tin số cá nhân và an toàn thông tin số cho hệ thống công nghệ thông tin chung của cơ quan nhà nước còn nhiều hạn chế.

- Hiện tổng số cán bộ chuyên trách công nghệ thông tin trong các cơ quan nhà nước là 278 cán bộ. Trong đó tỷ lệ cán bộ công nghệ thông tin có trình độ trên đại học là 13/278, trình độ đại học là 210/278, trình độ cao đẳng/ trung cấp là 55/278. Thành phố Hà Nội trong giai đoạn vừa qua chưa thiết lập được đội ngũ nhân lực chuyên trách về an toàn thông tin số của Thành phố trong khi đó tại các đơn vị số lượng cán bộ chuyên trách công nghệ thông tin chưa đủ đáp ứng yêu cầu cả về số lượng và chất lượng để tham gia công tác an toàn thông tin số tại các cơ quan nhà nước.

- Thành phố đã hoàn thành đào tạo nâng cao kiến thức về hệ thống thông tin và ứng dụng công nghệ thông tin trong cải cách hành chính cho 441 cán bộ chủ chốt của một số các đơn vị; các kiến thức chung về an toàn và bảo mật thông tin cho 300 cán bộ công chức các sở ngành, quận, huyện, thị xã. Tuy

nhiên số lượng cán bộ, công chức, viên chức được đào tạo về an toàn thông tin còn khá khiêm tốn so với tổng số cán bộ, công chức, viên chức của Thành phố.

Căn cứ kết quả khảo sát năm 2011, 2012 về đầu tư cho ứng dụng công nghệ thông tin của Thành phố. Trong đó, nguồn vốn WB thực hiện gói thầu xây dựng Trung tâm Dữ liệu nhà nước chiếm tỷ trọng lớn nhất (32,02%), tiếp đó là nguồn Chương trình công nghệ thông tin (chiếm 30,38%), ít nhất là nguồn chi thường xuyên và ngân sách đơn vị (chiếm 14,92%, không bao gồm đầu tư từ Trung ương và đơn vị của ngành Công an).

Năm 2011 và 2012, Thành phố đầu tư cho ứng dụng công nghệ thông tin khoảng 600 tỷ, trong đó đầu tư cho hạ tầng kỹ thuật của các huyện và các xã, thị trấn, các hệ thống thông tin và cơ sở dữ liệu, phần mềm ứng dụng dùng chung và các dịch vụ công mức 3 khoảng 88,87%; đào tạo chiếm 4,95%. Tuy nhiên, tỷ lệ đầu tư cho an toàn thông tin còn tương đối thấp chỉ khoảng 6,19%, chủ yếu thuộc nội dung đầu tư của các dự án về công nghệ thông tin.

Mặc dù các cơ quan nhà nước của Thành phố đã bắt đầu quan tâm đầu tư cho an toàn thông tin số, tuy nhiên mức đầu tư ban đầu đối với hoạt động an toàn thông tin số còn thấp so với tốc độ phát triển ứng dụng công nghệ thông tin của Thành phố, sự chênh lệch trên dẫn đến nguy cơ cao mất an toàn thông tin đối với cơ sở hạ tầng công nghệ thông tin và các ứng dụng đang triển khai trong Thành phố hiện nay.

## 6. Nhu cầu đầu tư cho an toàn thông tin số giai đoạn đến năm 2015

### 6.1 Kế hoạch đầu tư cho công nghệ thông tin theo chương trình mục tiêu 2012-2015

Đơn vị: Tỷ đồng

Lĩnh vực	2012	2013	2014	2015	Tổng
Hạ tầng	119,56	101,08	81,17	45,82	347,63
Ứng dụng	52,21	158,14	140,46	145,63	496,44
Đào tạo	1,00	3,00	3,00	3,00	10,00
Quản lý	8,14	12,35	10,58	9,16	40,24
<b>Tổng số</b>	<b>180,91</b>	<b>274,57</b>	<b>235,21</b>	<b>203,61</b>	<b>894,30</b>

### 6.2 Nhu cầu đầu tư cho an toàn thông tin số đến năm 2015

Xuất phát từ thực tế đã thực hiện cho an toàn thông tin số trong giai đoạn 2005-2010; tổng kết đầu tư năm 2011 cùng với mặt bằng và yêu cầu cần thiết phải thực hiện trong bối cảnh tình hình hiện nay đến năm 2015, để đảm bảo vận hành an toàn toàn bộ hệ thống thông tin, Thành phố cần nâng mức đầu tư lên 10% tổng chi phí cho các dự án thông tin thuộc chương trình mục tiêu với nguyên tắc như sau:

- Đầu tư trọng điểm cho hệ thống mã hóa, xác thực công khai của Thành phố.
- Đầu tư bảo vệ cho các rủi ro an ninh xuất phát từ máy trạm
- Đầu tư hệ thống giám sát, cảnh báo và đánh giá an ninh độc lập
- Đầu tư bảo vệ cho hạ tầng mạng
- Đầu tư bảo vệ cho các hệ thống thông tin, ứng dụng, cơ sở dữ liệu hiện có

e. Đầu tư cho đào tạo việc tuân thủ và đảm bảo an ninh

### **III. MỤC TIÊU**

#### **1. Mục tiêu chung**

- Đảm bảo cơ sở hạ tầng thông tin của Thành phố hoạt động ổn định, an toàn và bảo mật, giảm thiểu thiệt hại do sự cố an toàn thông tin số.

- Nâng cao năng lực bảo đảm an toàn, bảo mật thông tin cho cán bộ, công chức, viên chức của Thành phố.

- Tự chủ công nghệ và giải pháp về an toàn thông tin số phục vụ công tác triển khai các hệ thống thông tin tác nghiệp và các ứng dụng dịch vụ công thuộc Chương trình mục tiêu của Thành phố.

#### **2. Mục tiêu cụ thể**

##### **a) Về bảo đảm An toàn thông tin số cho các hệ thống Công nghệ thông tin trong nội bộ cơ quan nhà nước**

- 100% các ứng dụng dùng chung, 50% các hệ thống thông tin và cơ sở dữ liệu trọng điểm, các dịch vụ công trực tuyến được triển khai tại Trung tâm Dữ liệu nhà nước Thành phố đảm bảo an toàn, bảo mật dữ liệu.

- 100% các hệ thống mạng LAN của các sở, ban, ngành, UBND quận, huyện thị xã, phường, xã thị trấn và mạng WAN của Thành phố phải được trang bị giải pháp đảm bảo an toàn bảo mật nhằm đảm bảo toàn vẹn tất cả các thông tin chỉ đạo, điều hành truyền trên mạng.

- 100% các cuộc họp trực tuyến của thành phố trên hệ thống Họp trực tuyến của Thành phố đảm bảo an toàn thông tin.

- Đảm bảo an toàn thông tin số cho hệ thống Thư điện tử của thành phố Hà Nội (có tên miền là @hanoi.gov.vn).

- 100% các máy chủ và các máy trạm được triển khai áp dụng các giải pháp đảm bảo an toàn thông tin, chống virus và mã độc hại, được cập nhật thường xuyên các bản vá lỗi hệ thống.

- 30% các hệ thống thông tin của các cơ quan nhà nước phải có các thiết bị sao lưu dữ liệu và áp dụng các quy trình sao lưu dự phòng dữ liệu, chính sách ghi lưu tập trung biên bản hoạt động (log file) cần thiết theo yêu cầu và theo hướng dẫn của Bộ Thông tin và Truyền thông.

- 100% các cơ quan nhà nước có quy chế và thực hiện quy chế an toàn bảo mật cho hạ tầng thông tin tại đơn vị mình.

##### **b) Về bảo đảm An toàn thông tin số cho các hệ thống cung cấp thông tin công cộng và dịch vụ công**

- 100% Trang thông tin điện tử của các sở, ban, ngành, uỷ ban nhân dân các quận, huyện, thị xã có giải pháp hiệu quả chống lại các tấn công gây mất an toàn thông tin và có phương án dự phòng khắc phục sự cố đảm bảo hoạt động liên tục ở mức tối đa.

- 100% Các giao dịch điện tử trong các dịch vụ công mức độ 3 và mức độ 4 tuân thủ các tiêu chuẩn chất lượng về an toàn thông tin và có biện pháp bảo đảm an toàn thông tin.

### **c) Về nguồn nhân lực An toàn thông tin số**

- Xây dựng, hình thành mạng lưới đội ngũ cán bộ chuyên trách an ninh, an toàn hệ thống trong Thành phố, bảo đảm 100% cán bộ chuyên trách được đào tạo và cấp chứng chỉ theo chuẩn quốc tế về an ninh mạng.

- 100% Cán bộ chuyên trách công nghệ thông tin trong các cơ quan nhà nước được đào tạo cơ bản về an toàn thông tin.

- 100% Cán bộ lãnh đạo, cán bộ chủ chốt, công chức, viên chức của Thành phố nhận thức đầy đủ về an toàn thông tin, có kỹ năng bảo vệ an toàn dữ liệu cá nhân.

## **IV. NỘI DUNG**

### **1. Hệ thống mã hóa, xác thực công khai của Thành phố**

Xây dựng hệ thống quản lý thông tin người dùng và xác thực số trung tâm dành cho các hệ thống thông tin và ứng dụng dùng chung tại Trung tâm Dữ liệu nhà nước đồng thời cung cấp các dịch vụ xác thực dành cho phần mềm nghiệp vụ đồng bộ với các hệ thống xác thực của Chính phủ.

Triển khai cấp chứng thực số đến toàn bộ các bộ công chức của các cơ quan nhà nước Thành phố, xây dựng và bổ sung các module chứng thực người dùng cho các phần mềm đã triển khai đồng bộ với hệ thống xác thực trung tâm và quản lý thông tin người dùng tại Trung tâm Dữ liệu nhà nước.

### **2. Đầu tư bảo vệ cho các rủi ro an ninh xuất phát từ máy trạm**

Trang bị phần mềm phòng chống virus tổng thể, quản trị tập trung để trang bị cho các máy chủ, máy trạm của các cơ quan nhà nước Thành phố.

Xây dựng hệ thống thu thập báo cáo, quản lý thông tin báo cáo về hiện trạng an toàn thông tin số; đồng thời trợ giúp người sử dụng trong việc cập nhật các bản vá và phòng vệ trên máy trạm.

### **3. Đầu tư hệ thống giám sát, cảnh báo và đánh giá an ninh độc lập**

Trang bị hệ thống thiết bị và phần mềm thẩm định nguy cơ mất an toàn mạng, nguy cơ lỗ hổng ứng dụng dịch vụ bao gồm: mua sắm trang thiết bị máy chủ, máy tính chuyên dụng và các phần mềm thẩm tra nguy cơ mất an ninh mạng và ứng dụng nhằm có giải pháp phòng tránh nguy cơ mất an toàn thông tin hoặc phát hiện các lỗ hổng bảo mật và sửa chữa kịp thời.

Xây dựng hệ thống quản lý thông tin báo cáo về hiện trạng đồng thời trợ giúp người sử dụng trong việc cập nhật các bản vá và phòng vệ trên máy trạm, ứng cứu các hệ thống thông tin trong các trường hợp khẩn cấp.

### **4. Bảo vệ cho hạ tầng mạng**

Triển khai hệ thống an toàn thông tin tổng thể bao gồm tường lửa, thiết bị cảnh báo xâm nhập và các thiết bị an ninh cho mạng WAN của Thành phố, lấy trọng tâm bảo vệ cao nhất là Trung tâm dữ liệu nhà nước Thành phố.

Bảo vệ, đảm bảo an toàn thông tin số cho Trung tâm Tích hợp dữ liệu của Văn phòng UBND Thành phố đảm bảo mạng tin học của UBND Thành phố vận hành ổn định, thông suốt để phục vụ công tác chỉ đạo, điều hành của UBND Thành phố, kết nối với mạng truyền số liệu chuyên dụng của Chính phủ và Hệ thống thông tin giữa Thành ủy – HĐND – UBND Thành phố.

Đầu tư nâng cao năng lực hệ thống trang thiết bị lưu trữ mạng, sao lưu dự phòng thảm họa nội bộ cho các máy chủ và máy trạm.

#### **5. Bảo vệ cho các hệ thống thông tin, ứng dụng, cơ sở dữ liệu hiện có**

Thẩm tra an ninh tổng thể cho các hệ thống thông tin dùng chung và chuyên ngành của các cơ quan nhà nước: Triển khai quét, dò các lỗ hổng bảo mật, thẩm tra an ninh định kỳ cho các hệ thống thông tin dùng chung và chuyên ngành của các cơ quan nhà nước.

Kiểm định và nâng cấp an ninh định kỳ cho các ứng dụng dịch vụ công hiện đã triển khai của các cơ quan nhà nước.

Nâng cấp an ninh định kỳ theo chuẩn hiện hành đối với các trang thông tin điện tử, cổng thông tin điện tử của các cơ quan nhà nước Thành phố.

#### **6. Tổ chức diễn tập An toàn thông tin**

Tổ chức diễn tập An toàn thông tin hàng năm với sự tham gia của các cơ quan nhà nước thành phố Hà Nội nhằm nâng cao năng lực cho đội ngũ cán bộ làm công tác đảm bảo an toàn thông tin tại các đơn vị và tăng cường hoạt động đảm bảo an toàn thông tin số của các đơn vị trong địa bàn Thành phố.

#### **7. Đào tạo nguồn nhân lực An toàn thông tin số**

Đào tạo quản lý an ninh chuyên sâu cho các cán bộ chuyên trách công nghệ thông tin: Đào tạo cho các cán bộ chuyên trách về hệ thống, an toàn thông tin, kiểm định và kiểm soát tuân thủ. Hình thành đội ngũ cán bộ chuyên nghiệp về an toàn thông tin số và ứng cứu khẩn cấp của Thành phố.

Bồi dưỡng kiến thức cơ bản về an toàn thông tin số và tuân thủ quy định về an toàn thông tin số cho cán bộ, công chức, viên chức: Huấn luyện, bồi dưỡng kiến thức cho đội ngũ cán bộ, công chức, viên chức của Thành phố để tuân thủ và áp dụng các quy định.

Tổ chức các buổi hội thảo về an toàn thông tin số và tuân thủ quy định, tiêu chuẩn an ninh dành cho các cơ quan nhà nước và doanh nghiệp: Hội thảo về an toàn thông tin số, tập huấn về các quy định cho các doanh nghiệp phát triển phần mềm, tích hợp hệ thống nhằm tuân thủ các quy định về an ninh khi tham gia xây dựng hoặc chào thầu giải pháp đến các cơ quan nhà nước Thành phố.

### **V. GIẢI PHÁP THỰC HIỆN**

#### **1. Chỉ đạo, điều hành**

Ban chỉ đạo công nghệ thông tin Thành phố tăng cường chỉ đạo về an toàn thông tin số trong hoạt động của cơ quan nhà nước.

Tiếp tục hoàn thiện bộ máy quản lý nhà nước về an toàn thông tin số từ

cấp Thành phố đến các cấp sở, ban, ngành, quận, huyện, thị xã; trong đó chú trọng nâng cao năng lực của các cán bộ chuyên trách về an toàn thông tin số.

## **2. Giải pháp tài chính**

Phân bổ ngân sách đảm bảo đầu tư mới cho phát triển các hệ thống an toàn thông tin số hàng năm chiếm khoảng 10% trong tổng kinh phí chi cho Ứng dụng công nghệ thông tin của Thành phố, trong đó kinh phí chi thường xuyên hàng năm cho các công tác đảm bảo, giám sát và phát triển các giải pháp an ninh chiếm khoảng 30%.

Tập trung đầu tư các dự án, nhiệm vụ độc lập về an toàn thông tin số sử dụng nguồn vốn thuộc Kế hoạch bảo đảm an toàn thông tin số của Thành phố đến năm 2015 đã được phê duyệt nhằm đạt được các chỉ tiêu đã đề ra, tạo cơ sở pháp lý và nền tảng hạ tầng cho các giai đoạn sau này.

Các Sở, Ban, Ngành và các UBND quận, huyện, thị xã: trên cơ sở kế hoạch của từng đơn vị trong kế hoạch ngân sách hàng năm, phải có mục chi cho công nghệ thông tin về bảo đảm an toàn thông tin số để thực hiện các dự án công nghệ thông tin thuộc phạm vi của đơn vị; tự bảo đảm an toàn thông tin số tại đơn vị mình.

## **3. Giải pháp về triển khai**

Các hệ thống trung tâm, các cơ chế chính sách đã và đang được đầu tư sẽ là khởi điểm ban đầu để triển khai các dự án và nhiệm vụ thuộc kế hoạch này, lấy làm cơ sở để sau này nhân rộng đến toàn bộ các đơn vị khác trong địa bàn Thành phố.

Sở Thông tin và Truyền thông là cơ quan quản lý nhà nước chuyên ngành của Thành phố thực hiện chức năng, nhiệm vụ theo thẩm quyền (xây dựng chính sách ứng dụng và phát triển công nghệ thông tin trên địa bàn; hướng dẫn triển khai thực hiện; quản lý và đảm bảo hạ tầng dùng chung, các ứng dụng dùng chung...) và phối hợp với các cơ quan quản lý theo phân cấp trong công đảm bảo an toàn thông tin số.

## **4. Giải pháp kiểm tra, giám sát**

- Thường xuyên rà soát tiến độ triển khai kế hoạch bảo đảm an toàn thông tin số tại các cơ quan nhà nước của Thành phố.

- Tăng cường công tác kiểm tra định kỳ về an toàn thông tin số.

- Tổ chức đánh giá định kỳ và công bố các báo cáo hàng năm về năng lực đảm bảo an toàn thông tin số đối với các hệ thống thông tin quan trọng của Thành phố.

## **5. Giải pháp môi trường chính sách**

- Rà soát và hoàn thiện các văn bản quy phạm pháp luật, cơ chế và chính sách của Nhà nước cũng như Thành phố, tạo môi trường thuận lợi để đảm bảo an toàn thông tin số, đáp ứng các yêu cầu về hội nhập toàn diện kinh tế quốc tế, thúc đẩy hợp tác với các doanh nghiệp, tổ chức trong và ngoài nước trong lĩnh vực an toàn thông tin số.

- Xây dựng quy chế an toàn thông tin số chung cho các cơ quan nhà nước của Thành phố: Nghiên cứu và ban hành các quy định về quy chế, chính sách thực hiện đảm bảo an toàn, an ninh tuân thủ tiêu chuẩn an ninh theo tiêu chuẩn ISO27001 và tiêu chuẩn ISO19001.



- Xây dựng quy trình và các hướng dẫn thực hiện đảm bảo an toàn thông tin số trong nội bộ cơ quan nhà nước của Thành phố: Nghiên cứu các quy trình bảo mật và đảm bảo an toàn thông tin cho cán bộ quản trị hệ thống, nhân viên kiểm soát an ninh và người sử dụng hệ thống khi giao tiếp, trao đổi; Ban hành các quy chuẩn về hệ thống máy tính, trang thiết bị, máy chủ, phần mềm hệ thống, phần mềm nghiệp vụ ...

- Xây dựng tài liệu chỉ dẫn an toàn thông tin số, chỉ dẫn phát triển ứng dụng đảm bảo an toàn thông tin số cho các đối tượng người sử dụng, công dân và các doanh nghiệp phát triển phần mềm.

## **6. Nâng cao nhận thức**

- Tiếp tục công tác tuyên truyền rộng rãi nhằm nâng cao nhận thức của người dân, doanh nghiệp về lợi ích ứng dụng công nghệ thông tin và tầm quan trọng của việc bảo đảm an toàn thông tin.

- Đặc biệt chú trọng nâng cao nhận thức của người dân trong việc đảm bảo an toàn thông tin trong khai thác sử dụng Internet, trong các giao dịch dịch vụ công trực tuyến với các cơ quan Nhà nước, trong các giao dịch điện tử... để tránh thành nạn nhân mạng cũng như vô tình tiếp tay cho các hoạt động phi pháp của tội phạm mạng.

- Tăng cường hợp tác để học tập kinh nghiệm trong nước và quốc tế trong việc đảm bảo an toàn thông tin số.

## **VI. KINH PHÍ THỰC HIỆN**

Kinh phí thực hiện bằng ngân sách Thành phố cấp cho Chương trình công nghệ thông tin Thành phố và ngân sách của các sở, ban, ngành, UBND các quận, huyện, thị xã.

## **VII. TỔ CHỨC THỰC HIỆN**

### **1. Sở Thông tin và Truyền thông**

Là thường trực Ban chỉ đạo Công nghệ thông tin Thành phố có trách nhiệm tham mưu cho UBND Thành phố chỉ đạo công tác an toàn thông tin số trong hoạt động của cơ quan nhà nước Thành phố.

Hướng dẫn các sở, ban, ngành Thành phố, UBND các quận, huyện, thị xã xây dựng kế hoạch và triển khai thực hiện kế hoạch, dự án công nghệ bảo đảm an toàn thông tin số của đơn vị.

Tổ chức triển khai các nhiệm vụ đảm bảo an toàn thông tin số đối với hạ tầng mạng diện rộng của Thành phố, các hệ thống thông tin, ứng dụng, CSDL giao Sở Thông tin và Truyền thông chủ trì triển khai đặt tại Trung tâm Dữ liệu nhà nước.

Đề xuất cơ chế, chính sách, giải pháp ứng dụng công nghệ thông tin về bảo đảm an toàn thông tin số, đồng thời hướng dẫn và tổ chức thực hiện sơ kết, tổng kết tình hình thực hiện kế hoạch hàng năm.

Kiểm tra, giám sát, đôn đốc việc đảm bảo an toàn thông tin số trong các cơ quan nhà nước của Thành phố.

Phối hợp với Sở Kế hoạch và đầu tư, Sở Tài chính xây dựng dự toán kinh phí thực hiện các dự án công nghệ thông tin về bảo đảm an toàn thông tin số hàng năm trình UBND Thành phố xem xét, phê duyệt.

Định kỳ hàng năm, báo cáo đánh giá việc thực hiện kế hoạch của các cơ quan nhà nước với UBND Thành phố.

## **2. Sở Tài chính**

Phối hợp với Sở Thông tin và Truyền thông ban hành quy định về tài chính phù hợp đặc thù cho các dự án công nghệ thông tin về bảo đảm an toàn thông tin số trên địa bàn Thành phố.

Bảo đảm cân đối ngân sách cho các dự án công nghệ thông tin về bảo đảm an toàn thông tin số trên địa bàn Thành phố theo kế hoạch hàng năm đã được các cấp có thẩm quyền phê duyệt.

## **3. Sở Kế hoạch và Đầu tư**

Chủ trì, phối hợp với Sở Tài chính, Sở Thông tin và Truyền thông cân đối tổng hợp kinh phí đầu tư hàng năm cho các dự án công nghệ thông tin về bảo đảm an toàn thông tin số trên địa bàn Thành phố.

## **4. Sở Nội vụ**

Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các Sở, Ban, Ngành liên quan đề xuất các chính sách khuyến khích, thu hút cán bộ về an toàn thông tin giỏi; quy chế về việc đào tạo, bồi dưỡng đối với cán bộ chuyên trách về an toàn thông tin.

Phối hợp với Sở Thông tin và Truyền thông xây dựng các chương trình nâng cao nhận thức, phổ cập kiến thức về an toàn thông tin số cho cán bộ, công chức, viên chức các ngành, các cấp của Thành phố.

## **5. Công an Thành phố**

Phối hợp với Sở Thông tin và Truyền thông trong công tác phòng ngừa, đấu tranh, chấn áp các loại tội phạm công nghệ cao, gián điệp mạng, các nguồn phát tán virus, mã độc hại nhằm đảm bảo an ninh mạng và an toàn thông tin số.

## **6. Các Sở, Ban, Ngành và UBND các quận, huyện, thị xã**

Căn cứ Kế hoạch đảm bảo an toàn thông tin số của Thành phố giai đoạn 2013-2015, chủ động xây dựng, điều chỉnh kế hoạch và dự toán ngân sách cho các dự án công nghệ thông tin về bảo đảm an toàn thông tin số hàng năm gửi Sở Thông tin và Truyền thông, Sở Kế hoạch và Đầu tư, Sở Tài chính để tổng hợp, cân đối trình các cấp có thẩm quyền phê duyệt trong dự toán ngân sách hàng năm của các đơn vị.

Chủ động triển khai các nhiệm vụ đảm bảo an toàn thông tin số trong nội bộ từng cơ quan.

Kiểm tra, đánh giá và báo cáo định kỳ thực hiện Kế hoạch theo hướng dẫn của Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND Thành phố.

Trên đây là Kế hoạch đảm bảo an toàn thông tin số của Thành phố đến năm 2015, UBND Thành phố yêu cầu các sở, ban, ngành Thành phố, UBND

các quận, huyện, thị xã nghiêm túc triển khai thực hiện, định kỳ báo cáo kết quả với UBND Thành phố qua Sở Thông tin và Truyền thông để tổng hợp./.

**Nơi nhận:**

- Bộ TTTT;
- TTTU-TTHĐND TP;
- Đ/c Chủ tịch UBND TP;
- Các đ/c Phó Chủ tịch UBND TP;
- Văn phòng Thành ủy, VP HĐND TP;
- Các sở, ban, ngành, đoàn thể TP;
- UBND các quận, huyện, thị xã;
- VPUBNDTP: Đ/c CVP, đ/c PCVP Đỗ Đình Hồng, các phòng VX, TTTHCB, TH;
- Lưu: VT, VXh.

13

130

TM. ỦY BAN NHÂN DÂN

KT. CHỦ TỊCH

PHÓ CHỦ TỊCH



Nguyễn Thị Bích Ngọc

www.LuatVietnam.vn