DIRECTORATE OF LOCAL FUND AUDIT, ODISHA
TREASURY AND ACCCOUNTS BHAWAN, UNIT –III,
KHARABEL NAGAR, BHUBANESWAR
Ph. (0674) 2391704, e-mail ID-dirlfaodisha@gmail.com

****

DLFA-HE-I-17/2017

Memo No 7391 /DLFA dt 01.07.17//

Copy along with Copy of Letter No. 16440/F dt. 22.05.2017 and Letter No. 19527/F dt. 27.06.2017 of Govt. of Odisha in Finance Department & its enclosure forwarded to All District Audit Officers, Local Fund Audit in the State & Audit Officer, LFA, BBSR for information and necessary action.

01.07.17
Assistant Director

Memo No 7392 /DLFA dt 01.07.17//

Copy along with Copy of Letter No. 16440/F dt. 22.05.2017 and Letter No. 19527/F dt. 27.06.2017of Govt. of Odisha in Finance Department & its enclosure forwarded to All officers/ All Section / All Assistants/ ALFA Section/ of this office for information and necessary action.

01.07.17
Assistant Director

Memo No 7393 /DLFA dt 01.07.17//

Copy along with Copy of Letter No. 16440/F dt. 22.05.2017 and Letter No. 19527/F dt. 27.06.2017of Govt. of Odisha in Finance Department & its enclosure forwarded to Sri Trimurty Prasad Nayak, Jr. Programmer of this office for information and necessary action.

01.07.17
Assistant Director

5475
28.6.17 128

GOVERNMENT OF ORISSA
FINANCE DEPARTMENT
*****

28 JUN 2017

No. 19527 ., Dt. 27.06.2017
-FIN-BUD2-MISC-0006-2017

From
Sri S.P.Rath
Deputy Secretary to Government

To

Commissioner, Commercial Taxes, Odisha
Director, Treasuries and Inspection, Odisha
Controller of Accounts, Odisha
Director, Local Fund Audit, Odisha
Director, Madhusudan Das Regional Academy of Financial Management

Sub: *Implementation of Crisis Management Plan for Cyber Security in the State*

Sir/Madam,

I am directed to invite a reference to Letter No. 1995 Dated 19.06.2017 of Electronics and Information Technology Department, Government of Odisha (Copy enclosed) and to say that adequate steps may please be taken to meticulously follow the Guidelines annexed herewith to protect the Government Data system and to implement the cyber security best practices.

Yours faithfully

27/6/2017
Deputy Secretary to Govt.

29.6.17

Memo No. 19528 /F., dt. 27.06.2017

Copy along with copy of enclosures forwarded to Private Secretaries to Principal Secretary/ Special Secretaries/Additional Secretaries for kind information of Principal Secretary/Special Secretaries/Additional Secretaries.

29.6.17

27/6/2017
Deputy Secretary to Govt

Memo No. 19529 /F., dt. 27.06.2017

Copy along with copy of enclosures forwarded to all Officers /Branches for information and necessary action.

27/6/2017
Deputy Secretary to Govt

GOVERNMENT OF ODISHA
ELECTRONICS & INFORMATION TECHNOLOGY DEPARTMENT

No 1995 /E&IT
EIT-DEV-II-MISC-0001/2017

Bhubaneswar
Dated 19.06.17

From
Sri Ashok Meena, IAS
Commissioner-cum-Secretary to Government

To
All Principal Secretaries to Government /
All Commissioner-cum-Secretaries to Government/
Secretary, Works Department

Sub: Implementation of Crisis Management Plan for Cyber Security in the State.

Sir,

In continuation of this Department Letter No 1800 dated 20/05/2017 on the above noted subject, I am directed to send herewith a copy of "Compendium on Cyber Crime" prepared by CID, Crime Branch, Odisha and a copy of "Guidelines on Cyber Hygiene" for Secretariat IT users prepared by Head, State Portal Group for your reference.

Yours faithfully,

Commissioner-cum-Secretary to Government

Memo No 1996 /E&IT dated 19.06.17

Copy along with enclosures forwarded to P.S. to Chief Secretary/P.S. to D.C.-cum-ACS for kind information of Chief Secretary/ D.C.-cum-ACS.

Under Secretary to Government

Memo No 1997 /E&IT dated 19.06.17

Copy along with enclosure forwarded to Special D.G.P. (Crime) cum CISO, Cuttack /Head, State Portal Group, IT Centre cum Additional CISO for information and necessary action.

Under Secretary to Government

Guidelines for Cyber Hygiene

176

Objective

The objective of these guidelines is how to use good cyber hygiene for protecting and maintaining IT systems and devices appropriately by way of implementing cyber security best practices.

Overview of Cyber Hygiene

In the era of the digital age, everybody relies extensively on the Internet and electronic devices like Desktops, laptops, smart phones, tablets, and many more for both in work place and personal use, which is creating complexity in our IT environment, resulting in a lack of visibility and gaps in protection. Security measures are not keeping up with the volume, frequency, diversity, and sophistication of cyber attacks. Therefore the need to be proactive and vigilant to protect against cyber threats has never been greater. Government is no way an exception. Today, technology is driving more change in Government than ever before. To achieve security within the domain, we need to adapt a good cyber hygiene strategy, that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices for anything and everything that connects to the web, which includes

1. Organizing security in hardware, software and IT infrastructure
2. Continuous network monitoring,
3. Employee awareness and training.

Good cyber hygiene is built upon a robust vulnerability and threat management platform that enables user to continuously visualize the security posture of its IT infrastructure and better protect the official jobs against advanced cyber attacks.

Use of Cyber Hygiene in a network primarily requires awareness about the risks factors and possible origin of such risks and how to achieve immediate and effective defenses against risks. Hence objective of such awareness needs to focus on following points.

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Develop and manage secure configurations for all devices
4. Conduct continuous (automated) vulnerability assessment and remediation
5. Actively manage and control the use of administrative privileges

Guidelines

The Cyber Hygiene has to be bespoke at each of the following levels

1. End user Level

125

2. Gateway Level

3. Network Level

Adaption of Cyber Hygiene at End user Level:

End user Computing systems, mobile devices etc. are located in a distributed manner in a network. It is very difficult in normal circumstances that what software is downloaded, which external device is used by the user of the system. Hence ensuring Cyber Security of end user system is a challenging task. Any malicious activity at end user system may cause data loss, identity and data theft, malfunctioning of system, paralyzing the entire network etc.. In order to adapt security measures to ensure safe use of systems in the network following actions may be taken. In order to implement the following action points, the department should assign the task to a dedicated officer with proficiency in Information Technology

1. *Map the user with the Computing system and maintain an inventory of systems*

   Each and every system of the Department/office must be coded and an inventory specifying make, model, date of purchase, warranty, IP address, and MAC address of each system should be maintained. A register indicating code, user name should be maintained and updated in real-time basis. This will enable the Administrator to trace out a system in case of any incident happened in the network.

2. *Allow the end user to do the work as per his/her role.*

   It has been observed in most of the cases that, users download unnecessary software that may result in virus/malware infection in the system. At times system files are being deleted knowingly or unknowingly from the computer system that may result in hanging the system, nonfunctioning of system etc. Hence the Administrative privilege of computer system and Operating System of all the computers used within the Department should be with System Administrator of the Department only.

3. *Restrict the use of external devices at end user level.*

   Unless and until it is required the USB drives and DVD drives should be disabled in the system. This will help in controlling virus infection in the system as well as data theft.

4. *Ensure antivirus software is installed and running on the end user system.*

   All the systems in the Department/offices should have active antivirus installed. In Secretariat scenario, a Centralized Antivirus system is being implemented. All the Desktops and Laptops used for official use inside the secretariat must have this Antivirus installed so that user/department/office need not bother for updating of Antivirus as the same is being done centrally at IT Centre, Secretariat. All other existing antivirus software must be removed from the system.

5. *Ensure authenticated system software like Operating System, MS Office package etc. are installed in the system.*

Cases were found where user machine are having pirated Operating System, application software. Pirated software is Illegal. The pirated software do not update the patches released by the developer, which leads erratic behavior of the systems like system slowdown, virus infection etc.. Hence it is advised that Ensure that the computer system is having licensed Operating System and other application software like MS-Office etc..

6. *Ensure software patches are updated regularly.*

Update the software patches (most cases automatically done) to ensure security of the system.

7. *Do not allow third party software to be installed without prior permission of authority.*

Third pary software are unsafe in most cases. They may cause virus/malware infection. Most of the software installation requires administrative privileges on the system (O/S). Hence the System Administrator of the Department only has to have the Administrative privileges so that end user will not be able to install third party tools in most cases. However the administrator has to check periodically all the systems in thye department and clean the third party software is installed.

8. *Restrict access to the unnecessary and illegal websites.*

Department can install URL filtering solution in each desktop to avoid access to unauthorized sites. In Secretariat, a centralized gateway security system has been installed, which controls access to the sites centrally. It also monitors which site is accessed by which user at which time.

9. *Always allow user to access the network and internet through proper authentication.*

In order to access websites or intranet/internet applications within a Network (Intranet), a proper user authentication has to be ensured by way of implementing Active Directory. In Secretariat LAN, an Active Directory will be implemented shortly. Once Active Directory is implemented all users will be provided with an account for accessing the Internet/Intranet.

10. *Take regular back up of the system.*

The System Administrator has to take regular backup of the system in external drive to prevent data loss. The backup should be made through proper versioning with date and time stamp so that in case of eventuality data can be recovered.

Adaption of Cyber Hygiene at Gateway Level:

Each and every network has an interface that opens the same to public domain called gateway. The network has to be protected from Advance Persistent Threat, DoSS attacks, URL filtering, Content Filtering etc. at gateway level besides end user protection. Even if end user is protected

through Antivirus still it can be compromised by above mentioned threats. In Secretariat, Gateway Level Security has been implemented through Websense Content filtering solution.

Adaption of Cyber Hygiene at Network Level:

Each and every network has to be protected through a Firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS). This will protect the applications from intruders. In Secretariat, Network Level Security has been implemented through Check Point Next Generation Firewall Solution.

Short Guideline for suggested Activity

Guideline for new system.

1. Ensure that legal operating system and other software required for day to day operation are installed in the system.
2. Create an administrative user account.
3. Set up network connection(s).
4. Install browser in case same is not installed.
5. Install the **antivirus software**. In case the system is in the Secretariat LAN use the centralized Antivirus software in consultation with IT Centre. Install the device drivers for printer NIC etc. required for day to day operation.
6. Create a user account (Credential) for the officer who will use the system without Administrative privileges. In case multiple officers are going to use the system then create user account (credentials) for individual user.
7. Scan the entire system once with Anti Virus Software.
8. In case the external devices are not supposed to be used, then disable all of them.
9. Handover the user credentials to the respective users.
10. Periodically (**at least once in a month)** check the health of the system

(Action: Administrator of the Department/office)

Guideline for Daily use

1. Do not share your credentials to anyone.
2. Start the computer system using the user credentials given.

3. Change the password immediately in case the system is being used by the user for the first time. The password should be coined and updated as per following policy

   a. Minimum 8 characters to be used in the password.

   b. At least one Capital alphabet (upper case) , one numeric, and one special character (#,@, $ etc.) should be used while coining the password.

   c. Change the password in every month.

   d. While giving password do not use generic names like your vehicle name, so name etc.)

4. Run the antivirus in the system to scan the manually even though automatically scanning will be done at a particular time.

5. Do not try to install pirated software and insert external devices which are not at all required for official use.

6. Do not try to browse the illegal websites.

7. Do not change the network settings to access web through external network.

8. Scan the external device after inserting the same in to the system (Pen drive, CD/DVD etc.

9. Periodically delete all the temporary files.

10. Do not format the system. In case formatting is required the system administrator of your office may be contacted.

11. In case any vulnerability warning pops up or system gets slow then contact the System Administrator of your office.

4727
23.5.17

GOVERNMENT OF ORISSA
FINANCE DEPARTMENT
*****

No. 16440 ., Dt. 22.05.2017
FIN-BUD2-MISC-0006-2017/F

From
Sri S.P.Rath
Deputy Secretary to Government

To
Commissioner, Commercial Taxes, Odisha
Director, Treasuries and Inspection, Odisha
Controller of Accounts, Odisha
Director, Local Fund Audit, Odisha
Director, Madhusudan Das Regional Academy of Financial Management

Sub: *Implementation of Crisis Management Plan for Cyber Security in the State.*

Madam/Sir,

I am directed to invite a reference to Letter No. 1800 Dated 20.05.2017 of Electronics and Information Technology Department, Government of Odisha (Copy enclosed) and to say that a Crisis Management Plan for Cyber security in Odisha has already been notified by E & IT Department on 1st June, 2016, which can be accessed through the link http://appsit.odisha.gov.in/uploadDocuments/FormNotification/CMP-2016_Cyber%20Security_Odisha.pdf .

In view of the present RamsomWare Threat spreading widely across the globe, you are requested to take adequate steps to comply with the points raised for rigorous implementation of the said Crisis Management Plan for Cyber Security in the State.

Yours faithfully
22/5/2017
Deputy Secretary to Govt.

Memo No. 16441 /F., dt. 22.05.2017

Copy along with copy of enclosures forwarded to Private Secretaries to Principal Secretary/ Special Secretaries/Additional Secretaries for kind information of Principal Secretary/Special Secretaries/Additional Secretaries.

22/5/2017
Deputy Secretary to Govt

Memo No. 16442 /F., dt. 22.05.2017

Copy along with copy of enclosures forwarded to all Officers /Branches for information and necessary action.

22/5/2017
Deputy Secretary to Govt

120
105

Sh Ashok K K Meena, IAS
Commissioner-cum-Secretary to Government
& Chairman, OCAC

Government of Odisha
Electronics & Information Technology Department
OCAC Building, Plot No.N-1/7-D, Acharya Vihar
Bhubaneswar-751013, Odisha, India
Ph. No.: + 91-674-2567584 (O), Fax : + 91-674-2567842
Website : www.ocac.in, e-mail : itsec.or@nic.in

Letter No. 1800 /

Bhubaneswar
Dated 20/05/2017

To

The Development Commissioner-cum-ACS
All Principal Secretaries to Government
All Commissioner-cum-Secretaries to Government
Secretary, Works Department
All Revenue Divisional Commissioner, Odisha
All Collectors

Sub: Implementation of Crisis Management Plan for Cyber Security in the State.

Ref: This Department letter No.1751 dated 16/05/2017.

Madam / Sir,

As you know, the State Government is taking all possible steps to combat the present Ransomware Threat spreading widely across the globe. In this connection, necessary Advisory has already been sent vide this Department letter under reference and the same is also uploaded in the State Portal for wide awareness. A Video Conferencing with all the Collectors to review the preparedness was also held on 17/05/2017. The steps to be taken by the District Administration and Subordinate Offices to ensure protection of the critical Information Infrastructure at District level and down below were discussed in detail during this Video Conferencing. In this connection, I would like to intimate you that a Crisis Management Plan for Cyber Security in Odisha has already been notified by E&IT Department on 1st June, 2016. A copy of the Crisis Management Plan is enclosed herewith for your information and immediate implementation. The Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism outlines a framework for dealing with Cyber related incidents for a coordinated, multi-disciplinary and broad based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recovery from malicious Cyber related incidents impacting critical business functions and processes of Government of Odisha.

In the above backdrop. I would like to impressed upon all Departments and District Collectors to comply the followings:

1. **Survey of all Computer Systems and its upgradation.**

All Departments and Collectors to conduct a detail Survey of the Computer Systems available under their jurisdiction to ascertain it's vulnerability and to prevent the hacking of the same in future. During Survey the following basic parameters to be checked.

P.T.O

a. Whether updated Antivirus is loaded in the Computer System.
b. Whether latest Windows System with updated patches are installed in the Computer System.
c. Whether Pirated Software / Genuine Software is loaded in the System. If Genuine Software then the product Key number to be noted.

All Departments and Collectors after conducting the Survey must intimate the same to E&IT Department and upgrade the old computers with updated Operating System & Antivirus immediately at their end with the funds available with them or with support of the concerned Departments budget.

2. Incident Reporting Mechanism.

As per Para 5.2 of this Crisis Management Plan, when a cyber Crisis situation develops, respective Departments / District Collectors must immediately convey the same to this Department and also report the incident to CERT-IN in the manner and format as prescribed in Appendix –G of Cyber Crisis Management Plan.

3. Identification of Information Security Officer in each Department / Collectorate and Down below Offices.

As per the Crisis Management Plan all Departments, Directorates, Collectorates, Subordinate Offices and PSUs must nominate one Information Security Officer for their respective Department / Offices to coordinate with the Chief Information Security Officer of the State for any Cyber Security related issues. All Department and Collectors to ensure that the Information Security Officer of the respective offices under their control must be nominated immediately and their name, designation and contact details to be shared with this Department immediately.

4. Patch Updation.

The updated Patches and Windows Operating System issued by Microsoft is available in website of E&IT Department and the State Portal www.odisha.gov.in all Departments and District Collectors must ensure that this updated Patches are downloaded and updated in all the System under their Jurisdiction.

5. Awareness among the Government Official and General Public.

The E&IT Department is issuing Dos & Don'ts and Advisory to combat present Ransomware Threat in News Papers, Social Media and Government Websites. All Departments and District Collectors must ensure that these awareness messages are widely circulated among all Government Officials and General Public for their awareness. A copy of such Do's & Dont's is enclosed.

P.T.O

You are therefore, requested to comply the above points immediately and ensure that the provisions laid down in the Crisis Management Plan of the State is followed meticulously. The compliance report may be sent to this Department immediately. All Department to circulate this Guideline along with a copy of the Crisis Management Plan to the PSUs / Societies / other organizations under their Administrative Control with an instruction to comply the same immediately.

Yours faithfully,

20/5/17

Commissioner-cum-Secretary to Govt.

Memo No. 1801 /E&IT Dated 20.05.2017

Copy forwarded to PS to Hon'ble Minister, E&IT / OSD to Chief Secretary for information of Hon'ble Minister, E&IT and Chief Secretary respectively.

20/5/17

Commissioner-cum-Secretary to Govt.

Memo No. 1802 /E&IT Dated 20.05.2017

Copy forwarded to the Special DG of Police (Crime) and Chief Information Security Officer (CISO) / Head, State Portal for information and necessary action.

20/5/17

Commissioner-cum-Secretary to Govt.