REANDA
Biz Serve IT

ARE YOU WORKING FROM HOME?

Here are the 12 tips for control measures

WORK FROM HOME POLICY

JUNE 2020

General Background

Confidentiality, Integrity and Availability of information are critical to any organization for the on-going functions and good governance. It provides the guiding principles and responsibilities necessary to safeguard the security of the organization's information systems. Information systems of an organization must be secure at any cost and good policy helps to ensure this. Companies should be prepared for any type of worst situations like severe cyber-attacks, pandemics and natural hazards. They should have policies to ensure business continuity. One of such policy is Work From Home Policy which may also be referred to as Telecommuting Policy or Home-Based Work Policy.

The work from home policy aims to create and provide modern and efficient ways of working for employees from remote working location

The work from home policy aims to create and provide modern and efficient ways of working for employees from remote working location. But working from home / remote location, for many organizations, is a new concept and implementation of such phenomenon might be challenging. So every organization should tailor this policy as per their specific requirements.

Change in Information Security Strategy during Work from Home

ISO 27001 provides general guidelines for information security management system. Here, we are going to cover a brief summary of controls that should be taken care of during work from home environment and comply with ISO 27001 standard.

1. Security policy

Information Security Policy is a requirement under ISO 27001 and the policy should set out the security management system for the organization in relation to all forms of mobile working, including working from home. As every good security begins with the security policy, following policy statements must be considered prior to work from home.

Information Security Policy is a requirement under ISO 27001 and the policy should set out the security management system for the organization in relation to all forms of mobile working, including working from home

- **Who may work from home:-** identify the roles/jobs which may be considered for working from home.
- **Services available to staff:-** the type of network and application services which may be provided to staff working from home.
- **Information restrictions:-** are there any classified information which should not be made available to people working from home?
- **Identification/authentication/authorization:-** how should employees be identified, authenticated and authorized before accessing corporate resources from home?
- **Equipment and software specifications:-** are there any specific equipment or software products which must be deployed on the teleworker's PC before working from home? (eg. firewall or encryption software)
- **Integrity and confidentiality:-** consider how the connection to the remote PC should be protected (i.e. VPN) and how data on the machine should be protected.
- **Maintenance guidelines:-** how should the remote PC configuration be protected, updated and monitored?
- **User guidelines:-** clarify the user's role in protecting corporate resources- e.g., appropriate use of

resources; user should not modify security configurations; use of anti-virus software; storage of corporate data on local drives; use of encryption tools

- **User awareness:-** ensure that user understands the possible information risks associated with home users, how those risks are addressed, and the user's role in minimizing the risks.

2. Organization of information security

Employees must maintain adequate list of contacts of authorities that may be required during working from home. Also need to consider how the contact is to be made, by whom, under what circumstances, and the nature of information to be provided during work from home. Communication mediums such as mobile phone, email, collaboration tools, skype, etc. must be active. Also, assessment of risks while working remotely must be carried out prior to work from home.

Assessment of risks while working remotely must be carried out prior to work from home

3. Asset management

The assets management domain defines the controls for management of assets of an organization during the pandemic period. Inventory of assets must be in digital form so, the IT staff can use remotely. Any addition, change or deletion of information must be carried out through maker-checker controls. When working from home, employees should separate their office PC and personal PC. This may decrease the risk of being infected with a virus or malware. Employees using remote computing equipment must take precautions to ensure that they are working in a safe and secure manner. It's not recommended to use work devices to download personal apps or conferencing tools without IT approval. How and what Updates and patches are installed on employees personal computer must be defined. All connected hosts via remote access technologies must use the most up-to-date anti-virus software. Along with this, BIOS should be locked with password and hard drive should be encrypted.

It's not recommended to use work devices to download personal apps or conferencing tools without IT approval

4. Human resources security

The usual place of work or base for administrative purposes is usually the employees work desk. At the time of pandemic, this will be the employee's home. An employee whose job is feasible to work from home should be asked to complete a flexible working request. The working hours when the employee should be contactable and the attendance requirements for meetings and other office-based duties should be agreed and defined and communicated properly. They must be equipped with high-speed Internet, a Web camera, headset and collaboration software, so that employees can get in touch with each other at all time. An effective collaboration program should include such features as real-time video, high quality audio and presence detection systems.

The working hours when the employee should be contactable and the attendance requirements for meetings and other office-based duties should be agreed and defined and communicated properly

5. Physical and environmental security

Securing work environment is very important. Room should be designed as home office, if possible lock the door and ensure private conversations remain private by turning off Alexa and Google Assistant. To maintain clear desk policy all paper copies of sensitive information should be stored out of sight and

secure when not in use. If possible, shred when no longer needed. Screens should be locked when not in use and shut down all devices when the work is completed. While taking a break at home, work laptops should not be left unattended. Privacy screens should be used around friends and family and keep an eye out to avoid shoulder surfing. Staff should ensure that they are applying good moving and handling techniques when carrying portable equipment around home.

Staff should ensure that they are applying good moving and handling techniques when carrying portable equipment around home

6. Communications and operations management

Employees based at home should receive the same level of information, with the same frequency, as they were in office. Communication needs to be two-way, so it is important that open channels of communication are set up and maintained. Employees should not connect to public wireless or untrusted networks for work. Access to internal network should be connected via VPN only. These services should not be made accessible online in the name of remote work. VPN must be configured with adequate encryption and paraphrase. Network for these users must be segregated and heavenly monitored. Prior to work from home, the type of information and their communication channels must be clearly defined. Security must be employed according to the type of communication channel. Collaboration tools should be used to communicate between employees. The following questions that helps to select a collaboration tool that best meets organization's remote working needs:

Prior to work from home, the type of information and their communication channels must be clearly defined

1. Does the collaboration solution offer everything needed to work effectively from home, such as real-time document editing, audio, video, instant messaging, etc.?
2. Are all the necessary services integrated into one package or would we need to consider other alternatives (and expenses) such as conference calls for the audio?
3. Will the solution maintain total privacy and confidentiality of media and documents?
4. Does the system use a high level of encryption methods?
5. Does the system operate through firewalls? This is critical when communicating with external parties.
6. Is security included in the overall price of the solution, or is it an add-on cost?
7. Is education and training about how and when to use the service readily available and/or customized?

7. Access control

It is the responsibility of employees, contractors, vendors and agents with remote access privileges to its corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection. When accessing the network from a personal computer, Authorized Users should be responsible for preventing access to any computer resources or data by non-authorized users. If it's feasible Multi Factor Authentication should be enabled for all employees. Sensitive information such as credentials, access keys, 2 factor authentication devices, should not be laying around bed, table, floor, ceiling, ground, air, wind. Administrator or root users should not be accessible from internet, instead users should escalate their privileges if necessary. The authorized user bears responsibility for and consequences if there is misuse of the privilege. Employee should protect their login and password, even from family members. While using a device to remotely connect to corporate network, employees should ensure the remote host is not connected to any other network at the same time.

When accessing the network from a personal computer, Authorized Users should be responsible for preventing access to any computer resources or data by non-authorized users

8. Information systems acquisition, development and maintenance

When a new information system is acquired during work-from home period, it should be added into access control mechanism of the organization such as Active Directory and Firewall Access Control Lists. The logs that are generated by the system should be pushed to the logging server for the monitoring of illicit activities. Vulnerability Assessment and Penetration Testing should also be conducted on the system that is being acquired or developed.

The logs that are generated by the system should be pushed to the logging server for the monitoring of illicit activities

9. Information security incident management

A remote medium should be provided to the employees and contractors where they can report suspicious activities to the incident response department. If an information security incident takes place amid work-from home period, responsible department should be informed about it as quickly as possible. Classification and severity of the incident should be assessed, and responsibilities and procedures should be established by the department to provide effective and quick response. If authentication mechanism has been compromised, logging in should be disabled and the users should be required to force-change the password.

Classification and severity of the incident should be assessed, and responsibilities and procedures should be established by the department to provide effective and quick response

Mobile and email notification should be promptly alerted to the affected user-base. After the incident response, the organization should learn from it and implement proper authentication mechanism that will prevent the incident from happening in future.

10. Business continuity management

The organization should maintain security procedures to ensure the required level of continuity. Organization should be prepared with essential hardware, software, configuration and access management for change in security requirements in case of unexpected situations like lockdown imposed /extended due to COVID-19 pandemic, natural hazards like earthquakes, flood, land slide, fire, etc. Other essential equipments such as mobile phone with internet subscription, spare laptop, alternate connection system such as anydesk, Teamviewer, etc. must be defined and installed on respective users's PC.

The organization should maintain security procedures to ensure the required level of continuity

11. Compliance

Company should verify compliance to their policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

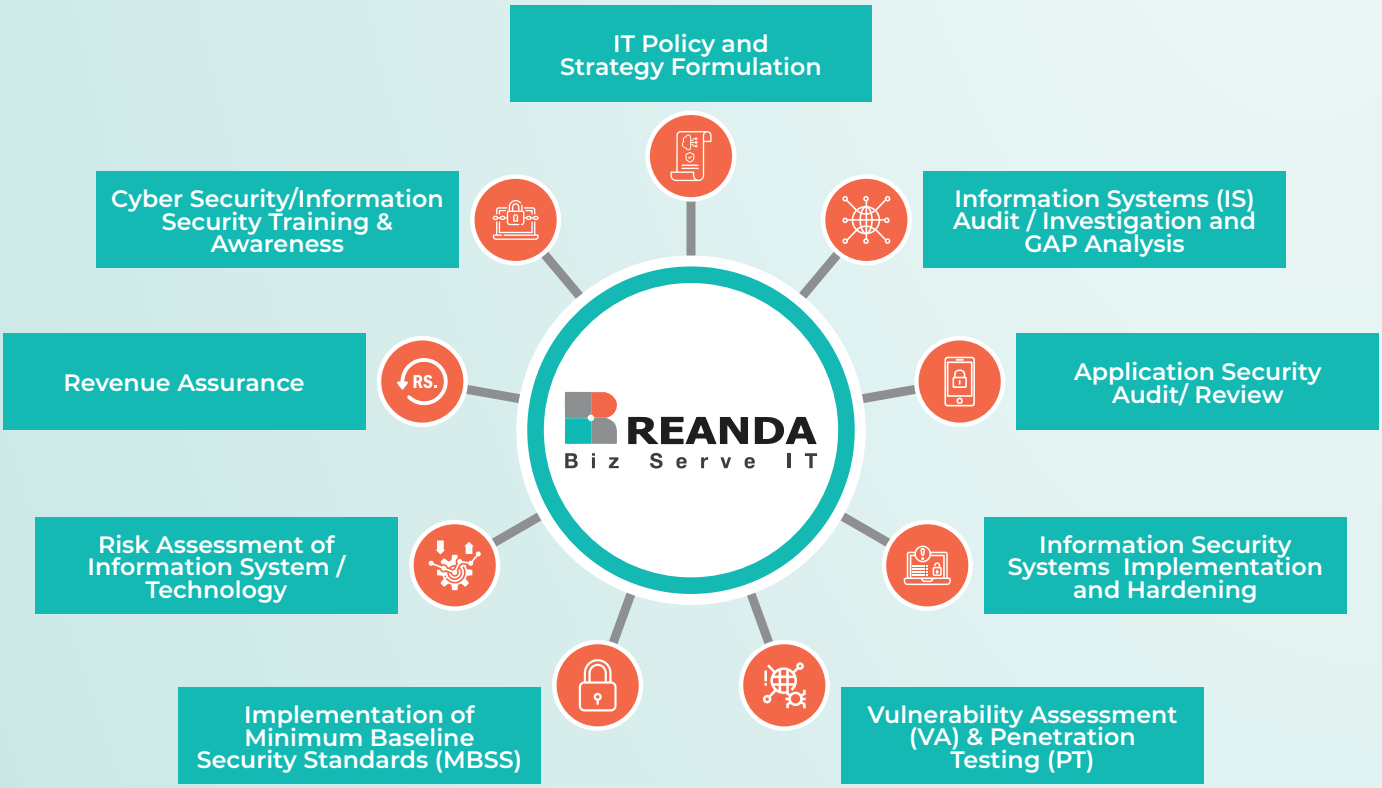
12. Awareness

Employees should be aware of phishing attacks. Avoid clicking on links in unsolicited emails and be aware of email attachments. Inspect links before clicking by hovering over links to see the actual URL destination.

Conclusion

Unexpected events are inevitable so we must always be prepared. With effective communication among colleagues, access control, heavy use of technology and time tracking system, work from home is effective. In this new working environment, the above controls could maintain same information security standard as normal working environment.

REANDA
Biz Serve IT



REANDA

Angola | Australia | Bangladesh | Belarus | Brazil | Cambodia | Cape Verde | China | Cyprus
Egypt | Germany | Greece | Hong Kong | India | Indonesia | Italy | Japan | Kazakhstan
Macau | Madagascar | Malaysia | Malta | Mauritius | Mozambique | Nepal | Netherlands
New Zealand | Pakistan | Poland | Portugal | Romania | Russia | São Tomé and Príncipe
Singapore | Taiwan | Ukraine | Turkey | UAE | UK | Vietnam

Contact US

Level 6, Sunrise Bizz Park
Dillibazar, Kathmandu

+977-1-4413535

bizserve@bizserve.com.np

www.bizserve.com.np
www.reanda-international.com