

Appendix 1

Undertaking of Data and Information Confidentiality and Security

For the purposes of maintaining the security and confidentiality of data and information in the entity, regardless of its source or nature, and whether that information is kept on paper, computer or any other means.

Based on the provisions of the Human Resources Law In the Federal Government, and its executive regulations thereof, remote working system, laws, regulations and instructions for the use of the intranet and internet, and pursuant to Cabinet Resolution No. 21 for 2013 regulating information security in the Federal Government, **I undertake to recognise and abide by the following:**

- All information, data and programmes of my entity, whether stored on hard disks, attached to an email message or any other form, are the property of the entity and the Federal Government.
- Using the entity's information is subject to federal laws and ethical considerations.
- Accessing any financial or administrative information obtained in the context of executing my duties is protected by the UAE laws, which I have to abide by.
- I will be granted access to the entity's information system, the "Bayanati" system, or any other system, the Internet, and e-mail for business purposes only.
- A breach of any of the information and data sources is considered illegal, as all data and information, including those obtained from outside the entity, are subject to regulations that prohibit copying and using such software.
- The entity is implementing the federal copyright laws that categorically prohibit any violation of these copyright laws.
- That the entity has systems and programmes to monitor and record all information systems, the Internet, and the use of e-mail. I am aware that these protection systems can register every website on the network that I have visited, as well as advertisements, incoming and outgoing email messages, files, information, and data that have been transferred from within or outside the entity. I am also aware that the entity is regularly checking information systems and internet activities and analysing their usage methods, and it will take the necessary measures in case of inappropriate use.

I also recognise that it is prohibited to:

- View, copy, or otherwise disclose confidential information of the entity to any Third party, unless that is part of my job and an official assignment.
- Change, delete, destroy or dispose of any confidential information for any reason, without obtaining written consent of the concerned officials in the entity.
- Discuss any confidential information with anyone other than concerned officials in the entity.
- Disclose any confidential information during my service or even after the termination of my employment at the entity.
- Share my passwords with other individuals or employees or use the entity's information systems using passwords of other employees.
- Leave laptops (iPad, memory chips, portable storage systems, etc.) in unsafe locations.
- Use illegally-obtained software.
- Install new software, or make changes to existing ones, whether hardware or software.
- Download programmes from the internet without the consent of the entity's IT department.
- Take no actions that interfere with the work of others, the network function, or any other computers.
- Use data, information and software for commercial interests or personal purposes.
- Send messages, files, programmes, or other connections that contain personal insult to others.
- Take no action that may adversely affect the rights of employees or disclose their personal information, or their financial benefits.
-

In order to protect confidential information, I undertake to:

- Keep my login details and passwords secret, change them regularly, and not disclose them to anyone else.
- Protect my computer applications from entering by anyone who is not authorised to do so by logging out of the programme or any other way to ensure protection.
- Carefully make all arrangements that ensure safe use and confidentiality of information when using the entity's systems according to the license granted to me to access the approved electronic systems.

- Inform my entity immediately upon my knowledge or reasonable suspicion, that the password has been infected with a virus or used by unauthorised persons, or upon suspicion of any activities that might violate the protection and confidentiality policies.
- Always use a safe work environment and act in the interest of the entity.
- Assume that the data may be read by persons other than those to whom it is sent.
- Take all measures of protection against viral infections and access by unauthorised persons to view the entity's data.

I understand and recognise that if I fail to comply with the terms of this undertaking and/or breaching the approved information security system, I will be held legally accountable, in addition to disciplinary liability by the entity, which has the right to decide the appropriate penalty without prejudice to any punishment in accordance with other laws and regulations.

By signing this undertaking, I acknowledge the compliance with all the statements and provisions contained therein, subject to legal liability.

Employee's Name:

Job No:

Job Title:.....

Appendix 2

Undertaking Not to Enter Into Subcontracts to Complete Tasks

I, the employee..... Work in a ministry /entity As (job title)..... Under the Remote Work System undertake to complete all the tasks assigned to me by my entity on my own without asking or authorizing any legal or material person to complete it on my behalf, or contracting others on this matter, and in case of breaching this undertaking I will bear legal responsibility for the consequences resulting from such breach towards my entity and the Federal Government.

Name:

Signature:

Date: