Republic of Rwanda
Ministry of ICT and Innovation

RISA
Rwanda Information Society Authority

REMOTE WORK GUIDE FOR GOVERNMENT EMPLOYEES

The Covid-19 global pandemic has evolved with astonishing speed, demanding swift action from all of us. In times like this, we are reminded of our inter-connectedness and the responsibility to each other. But most importantly, we are reminded of the opportunities Technology and digital tools present us as we continue to find ways of remaining productive during such a crisis. This remote work guide provides a set of guiding principles as well as the support that the Government of Rwanda has put in place to facilitate public service to continue with minimal disruption.

Guiding Principles:

1. Connected at all times during official working hours

a) Working remotely requires that **all staff remain available online** both on email and other remote work tools provided as well as Phones.

b) All employees are required to **check their emails regularly and respond** quickly, to allow for work to continue and decisions to be made in a timely manner.

c) Institutions **MUST** ensure that staff required to be connected are provided with Laptops and Internet bundles to enable them to work remotely. The recommended daily minimum bandwidth for each staff **is 3mbps.**

d) Everyone should be on standby and ready to report to their respective public institutions whenever requested by respective manager/direct report.

e) It is important to make a deliberate effort to connect frequently with all team members using any of the provided tools.

2. Meetings

a) All meetings including Senior Management Meetings (SMM), inter-institutional meetings, should be conducted virtually using either Zoom, Webex or Microsoft Teams. The IT teams within each institution will provide the required to support.

b) Online collaboration tools have been availed to IT teams in all institutions to facilitate remote work. Virtual meetings are encouraged using the following tools Below are links to tutorials on how to use these tools:

i. Zoom

https://support.zoom.us/hc/en-us/articles/206618765-Zoom-Video-Tutorials

ii. Webex

https://www.webex.com/webexremoteessentials.html

iii. Microsoft Teams

https://docs.microsoft.com/en-us/microsoftteams/tutorial-meetings-in-teams

https://static1.squarespace.com/static/59bbe92546c3c4cbf242e01c/t/5be2efe46d2a73f5ebef4fe6/1541599211825/Teams+Training+Guide.pdf

3. Physical Mail

f) Physical delivery of mail is discouraged. All institutions should publicly communicate an email address to which important letters and documents from the public should be emailed.

g) Public institutions are encouraged to use the document tracking and Workflow Management system, **e-Imboni**, to exchange mail between government institutions.

h) Central Secretariat team will continue to receive and dispatch mail electronically through the use of email and e-Imboni systems.

i) Email is highly encouraged as an official medium of communication.

4. Stay Safe Online

During this period where we are increasing working remotely leveraging digital tools to ease communication and collaboration, **exercising online safety is a MUST**. Stay safe online by paying attention to the following measures:

a) ***Safe use of passwords**:* Never share your password with anyone. We remind everyone that a strong password has at least 8 characters, which is a random sequence, including Lowercase letters, at least one Uppercase letter, at least one number, and at least one special character e.g. M!n@ICt2050#. Please do not use the same password for multiple important services, make sure you have different passwords on different accounts and change your passwords regularly (at least once in 3 months).

b) ***Safe use of Wi-Fi networks**:* Do not connect to open and occasional unsecured networks. It's essential to connect only to known and trusted networks. **The home/private Wi-Fi password should be changed from the manufacturer's default password to a new and more complex one with special characters** – a hard to guess password e.g. P@$$W0rd. Employees should not connect to public Wi-Fi to access work-related accounts such as emails and other documents.

c) ***Institutions that's have access to a Virtual Private Network (VPN),*** should use it to remotely connect to the corporate network via internet and to access internal resources or services. Staff will be provided with a

VPN account with credentials and a VPN client tool installed on their laptops.

d) ***Safe opening of emails, links, and attachments****:* Never open emails, links and attachments from any strangers or unknown suspicious sources. All employees should not visit untrusted websites, download movies on work computers or follow links provided by unknown or untrusted sources. All staff should be careful not to let anyone use/insert a USB drive on a corporate machine.

e) ***Safe use of the computer****:* It is recommended to lock your screen when not using it or log off your personal computer after you finish working and do not leave your laptop unattended.

f) ***Information security****:* Do not share personal or financial information on email or suspicious websites.

g) ***Backup****:* it is recommended to backup your data regularly. At least daily. Please ask your IT officers to assist you to back up your data while working from home.

h) ***Internet connection****:* While using video conferencing tools, **1.5Mbps** internet speed is the minimum recommended to ensure no disruption.

5. Daily priorities - Get ready for your work day as you would if you were coming into the office

a) It is important that supervisors and managers set their weekly priority tasks that get distributed to their team members.

b) Supervisors/Managers should engage their teams to ensure that daily and weekly priorities are communicated and reported on regularly through email or available collaboration tools.

c) Stay focused on the highest priorities. Keep your Daily work priorities top of mind and have regular check- ins with your manager to align on the most important work and deliverables.

d) Each manager/supervisor is required to check-in with their team members daily to ensure that priorities are adhered to and that relevant updates and/or information are shared in a timely manner.

6. Make an extra effort to get aligned and informed

It's a team effort, so proactively help your manager and team create structures and routines to:

a) Let others know what you are working on;
b) Stay informed on relevant projects and updates; and
c) Take time to learn how to effectively use the suite of tools that enable virtual team work: **Microsoft Teams, Zoom and webex**.

7. Support

IT teams of each institution will be available to provide the necessary support for setting up and using tools provided.

Below are the numbers for the IT team at RISA that will support you. They will work with your technical teams to get all the participants connected remotely.

S/N	Name	Email	Telephone number
1	Edson Mugabo	conference@risa.gov.rw	0788471778
2	Vincent Mucyo		0788445018
3	Morris Mwizerwa		0783123867
For Escalation			
	Alphonse zigira	Alphonse.zigira@risa.gov.rw	0788303645
	Josephine Nyiranzeyimana	Josephine.nyiranzeyimana@risa.gov.rw	0788545664