Guidelines

Collaboration and Work from Home Guidelines for IT Administrators

Version 1.1

Issue Date: 19 March 2020

PO Box 26662, Abu Dhabi, United Arab Emirates
www.tra.gov.ae

Table of Contents

1. Introduction

Online meetings and collaboration tools started to become important tools for everyday business in light of efforts to increase productivity, capitalize on ICT investments, reduce costs and reduce time.

There are varieties of tools in the market including Cloud-based on premise.

The purpose of the document is to introduce the security aspect and guidelines for deploying and using online meetings and collaboration tools. These guidelines improve the security and trust of the tool.

2. Scope

These guidelines are targeting all government entities users using collaboration and work from home tools such as Microsoft Teams, Zoom, Cisco Webex, Cisco Jabber and others.

3. General Collaboration Usage Guidelines

These Guidelines are general and applicable on On-prem and Cloud Based solutions.

Entities must advise their collaboration and work from home users the following:

- do not upload or share any mean of attachment without scanning the file for Viruses or Trojans.
- Do not use work-related Collaboration Tools for personal use.
- do not share files from unknown sources.
- do not accept any invitations from unknown users.
- report any suspicious activity to your system administrator immediately;
- do not record or screenshot conversation without all parties' permission and in accordance to the admin/entity policy.
- For meetings that require the enabling of the webcam, please ensure you are following the official dress code.
- Employees utilizing the platforms provided must be comply with acceptable use, ethical standards, and other TRA corporate policies when utilizing these platforms.

- The platforms are considered an official channel and should be used as such. The use of these platforms to spread hateful content, indecent content, and explicit language will be referred to Human Resources for a violation, warning, or more extreme measures based on the case.
- Please note that the security and compliance team have the capability of monitoring the usage to prevent the spread of malicious content such as virus that could be harmful to the entity's IT environment.

4. Public Cloud-Based Collaboration Guidelines

When intended to use Cloud-based Collaboration tools such as Microsoft Teams, the following additional guidelines must be advised to users:

- do not share confidential data through voice, document, video or any mean of communication;
- Confidential data can be shared only using On-prem solutions.

5. Guidelines to Administrators on specific platforms:

5.1. Microsoft Teams:

When intended to use the Microsoft Teams the following guidance must be considered:

- do not sync your internal Active Directory (AD) with Azure Active Directory;
- ensure that your organization Data Residency location is United Arab Emirates. If this is a new License you should choose UAE a data residency location. If this is old account (prior to 2019), then you may need to migrate your data to be in the UAE.
- enable Microsoft Multi-Factor-Authentication whenever possible.
- Enable Self Password reset to your employees to minimize support efforts.
- Assign Exchange Online plan to users to view Teams calendar.
- Advise your team members not share confidential data over Teams posts.
- Restrict Sessions Recording to authorized members only.
- Restrict Main/Public Organization Team Posts to authorized members only.
- Restrict Guest access to your Other organization teams and channels.
- Restrict Teams & Channels creations to teams owners with MS Teams lockdown.

- Monitor user access from Azure AD logins.

5.2. Cisco Jabber:

- Account authorization should be from Active Directory (AD) only.
- Restrict Cisco Jabber access through VPN.
- Additional guidance for use over the Internet without VPN.
    - In order to enable it over the Internet (without VPN), you must follow strictly Cisco deployment guidelines and Best Practices documents.
    - Server certificates should be signed by a trusted CA
    - Use encrypted protocols such as (https, srtp, srtcp)
    - ensure incoming connections are logged (example via syslog)
    - monitor/log CDR (Call Detail Records) to detect misuse.
- For mobile use, restrict IP address to reach the server and using given credentials (e.g. allow UAE based IP addresses only to reduce risks of attacks from outside the country)
- Install Cisco Jabber from internal repository.
- Pull all user in call manager from AD after integrating with AD.
- While configuring phone extensions on call manager bind specific user to the assigned extension.

5.3. Webex:

- Integrate Webex with AD so that only authenticated users are allowed.
- Pull all user from AD after integrating with AD.
- Provision external webex services in DMZ facing internet.
- Provision only https services for external Webex server with only parameter facing firewall.

5.4. Avaya Workplace:

- Integrate Avaya Workplace with AD so that only authenticated users are allowed.
- Pull all user from AD after integrating with AD.
- Provision external Avaya Workplace services in DMZ facing internet.
- Provision only https services for external Avaya Workplace server with only parameter facing firewall.

6. Non-compliance:

These are voluntary guidelines however, Non-compliance may result in unnecessary security, legal and financial risks. This may include violation against UAE Law, TRA Policies, Information Assurance Standards, UAE Government IT Policy and HR policies