# PRIVACY & SECURITY FOR WORKING REMOTELY

## PROTECT CONFIDENTIAL INFORMATION

1. If others are in your home, keep your work in the most secluded, secure place, like a closed room
2. All information that is not officially public is confidential, particularly if it is about identifiable individuals, including student records, grades, and most HR and financial information
3. Only share confidential information with faculty or staff who need it for University work

## ELECTRONIC RECORDS – FILES AND DOCUMENTS

1. Ensure devices have up-to-date security, including firewall, patches, anti-virus and anti-spam
2. Keep confidential information on secure University systems; not on home devices
3. Encrypt information you can't keep on secure University systems; eg. on an encrypted USB key or drive
4. Access work, files, and documents only on authorized, secure University systems with encrypted connections to MS Teams, O365 email, & approved apps
5. Protect all of your devices, accounts and log-ins with strong passwords
6. Logoff systems when you are no longer using them
7. Lock or shutdown devices when you leave, and set all devices to lock after 5-10 minutes of inactivity

## PHYSICAL RECORDS AND MEDIA

1. Protect files and documents from all unauthorized individuals, including family and friends
2. If others are in your home, keep your work in the most secure place, such as a closed room
3. Put files and documents away when not in use; if you can, in a locked cabinet, in your locked home
4. Take as few files or documents as you need for offsite work; if possible, copies instead of originals
5. Carry files and documents in a locked bag or case if you have a lockable one
6. Never leave files or documents unattended - in a car, restaurant, or on public transit, etc.
7. Never open/read files or documents where others could see or "shoulder surf"
8. Securely destroy hard copy files, documents, and physical media by crosscut shredding them

## PROFESSIONAL RECORD KEEPING

1. Continue to make your official communications professional and excellent
2. Use a separate message for personal messages, such as concerns, personal greetings, or jokes
3. Follow University of Toronto Archives and Records Management policies and procedures

## PRIVACY AND SECURITY PROBLEMS

- If you suspect a security problem or issue, immediately contact your IT help desk
- Privacy issues; immediately contact the Freedom of Information and Protection of Privacy Office (FIPPO)

## FOLLOW THE EXCELLENT UNIVERSITY REMOTE WORK, SECURITY AND IT GUIDANCE AT:

IT security, Records Management, Human Resources, Video Conferencing, Educational Technology, and ITS

**The FIPP Office is working remotely. Please call or e-mail us for privacy or access questions**:


**Rafael Eskenazi**
Director, FIPP Office
office: 416-946-5835
mobile: 416-427-4963
rafael.eskenazi@utoronto.ca

**Kelly Carmichael**
FIPP Coordinator
office: 416-946-7303
kelly.carmichael@utoronto.ca

**Lindsay Mills**
FIPP Coordinator
office: 416-978-4873
lindsay.mills@utoronto.ca