ACTION IN THE EVENT OF AN INFORMATION SECURITY (CYBERSECURITY) INCIDENT

RIGA GRADUATE SCHOOL OF LAW

1. ASSESS THE INCIDENT AND STOP SUSPICIOUS ACTIVITY

- If you notice suspicious emails, unusual system behaviour or other irregular activities, immediately stop interacting (e.g., do not click suspicious links or open attachments)
- If you identify physical device tampering or unauthorised access (e.g., unknown devices or restricted area access), do not interfere and report it

2. REPORT THE INCIDENT TO IT SUPPORT

Immediately contact IT Support and provide:

- type of incident (e.g., suspicious email, unauthorised access);
- time when the incident was noticed;
- all available evidence (screenshots, emails, system messages, etc.)

3. PROTECT DEVICES AND DATA

- If safe and appropriate, disconnect the device from the network (Wi-Fi or Ethernet) to reduce further impact
- Do not power off the device if IT specialists may need to investigate the incident

4. DOCUMENT ALL INCIDENT DETAILS

- Record all important events and actions from the moment the incident was detected
- Note times, actions taken and observations
- Preserve evidence that may support investigation

5. FOLLOW COMMUNICATION RULES

- Do not share information about the incident beyond IT specialists or authorised personnel
- Avoid spreading unverified information to prevent panic or misinformation
- Follow confidentiality requirements

6. FOLLOW IT INSTRUCTIONS AND COOPERATE WITH THE INVESTIGATION

- Cooperate with IT Support and provide requested information
- Follow instructions regarding system checks, password changes or other security measures

7. REVIEW PASSWORDS AND ACCESS RIGHTS

- Change passwords for affected systems or accounts when instructed by IT specialists
- Review assigned access permissions and ensure they match your responsibilities

MAIN IT CONTACT AT RGSL: KETIJA JŪLIJA BERGA (67039334, SUPPORT@RGSL.EDU.LV)

MAIN EMERGENCY CONTACT AT RGSL: IMANTS JEVDOKIMOVS (29244834)