Summary Document

CU IT Security Policy

Office of Information Technology, Chulalongkorn University

This document constitutes Chulalongkorn University's Information Technology Security Policy as the guidelines for faculties, colleges, offices, centers and operational units at all levels. It is issued by Office of Information Technology, Chulalongkorn University.

This is to ensure that the information technology infrastructure, data, network, hardware and software managed by the University are appropriately secured in order to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. Failure to adequately secure information increases the risk of financial and reputational loss to the University. Scope of this Policy provides a framework for the management of information security throughout the University in 10 aspects as follow:

1. **Policy and guidelines for IT Physical Security (Page 3-6)**

Focuses on directions to protect and monitor the safety of physical infrastructure, computer server room and server building. Mentions authorization, access control, incident management, disaster recovery, human error prevention, and burglary protection.

2. **Policy and guidelines for Network Security Preparedness (Page 7-9)**

Includes requirement for application or hardware testing as well as work mandate at pre-installation, installation, and post-installation process.

3. **Policy and guidelines for Information classification and management (Page 10-20)**

Mentions policy, regulation, and practices for information management, namely confidentiality and sensitive information management, data accessibility, data discovery, data transferring, data storage, data duplication, data removal and deletion.

4. **Policy and guidelines for Data backup and recovery (Page 21-22)**

Explains process of data backup and data recovery as to mitigate risk. Includes compulsory actions for data backup system that must be applied at every operational units. Mentions fault logging report that requires IT administrator to report any errors found from data backup along with

corrective measures, progress report and executive summary. Addresses data recovery plan which requires the latest update data retrieval. If the failure effects user service, IT administrator must notify users and keep recovery progress informed until the resuming the normal operation.

5. **Policy and guidelines for Change Management (Page 23-25)**

Gives instruction and to-do list before changes of information system applied in order to mitigate risks of IT service termination, as well as to allow IT administrator and users plan and prepare to handle consequence of the changes. The changes include patch update, process changes, operational system changes.

6. **Policy and guidelines for Computer Network Management (Page 26-30)**

Covers IP Address management, IP Address assignment, guidelines for network administrators, daily computer network monitoring, network performance monitoring, remote computing, system security, maintenance, and bandwidth monitoring. Includes contingency actions for computer systems or network system downtime and power outage.

7. **Policy and guidelines for Information System Accessibility (Page 31-33)**

Explains how the organization manage the cyber security and control information accessibility to reduce the risk of being affected by cyber crime .

8. **Policy and guidelines for the use of personal device (Page 34-36)**

Introduces how university students and staffs could use personal devices or office devices safely (i.e. smartphones, laptops, tablets, computers) when connecting to the university's internet or intranet. Focuses on personal cyber security to reduce the risk of being affected by cyber-attack, personal data intrusion, computer virus, malware, Trojan, etc.

9. **Policy and guidelines for Computer and Networking Ethics (Page 37-38)**

Explains moral principles that govern the usage of computers, internet, university's network and intranet for faculties, students and staff. Focuses on proper use of information technologies with respect to cyber morals, ethics, law, personal data privacy, university's confidentiality, the rights and property of others on the Internet, and university reputation.

10. Policy and guidelines for Business Continuity Plan (BCP) and Disaster Management (Page 39-40)

Details Business Continuity Plan (BCP) of Chulalongkorn University IT System to ensure IT service continuity. Includes execution plan in accordance with incidents and level of severity, and responsible persons. 4 Major topics cover:

- IT risk assessment
- IT risk mitigation and action plans
- Contingent resources and budget
- Annual BCP rehearsal and revision