APU-Net Guide	Ver	Operating System
APU Information Systems **Policy and User Guide for Network Security and Privacy**	1.0	All users

Introduction

This document stipulates the policy and guidelines for the usage and security of computer systems and networks at Ritsumeikan Asia Pacific University (APU).

The following guide applies to all members of the university who use its resources for teaching and research.

Guide

Prohibition of Unauthorized Access

When using the network, you are forbidden from attempting to gain unauthorized access to the system or illegally access another person's account.

Restrictions on Programs and Homepages that Require Password Authentication

For the sake of security and to protect personal information, you may not use programs that ask for user account names and passwords or other online fill-in forms on the APU-Net system. If you need to employ user authentication, which permits users access to a certain area, please contact the Information Systems Office.

Prohibition of Sharing User Accounts

Users are identified on the system by their user names and passwords and can access their personal data. For this reason, you are not permitted to share you user account with another person, transfer your user account to another person, or let another person use your account. If you would like to share a user account and password with someone else, please contact the Information Systems Office.

User Responsibilities

APU-Net users are responsible for using their accounts properly. Prevent information leaks by avoiding passwords that can be easily guessed by someone else (e.g., your name or date of birth) and by changing your password regularly.

Also be aware that it is easier for someone to steal your password and abuse your account if you write it down on a piece of paper or in your daily planner.

Ensuring System Security

All students, faculty and staff at APU are responsible for take ample security measures when attempting to connect to the APU-Net system.

For example, if your personal computer gets infected with a virus, worm or other piece of malicious software, it can attack the network and other systems connected to it. When an infection or attack

Last updated: 2014/9/30

APU-Net Guide	Ver	Operating System
APU Information Systems **Policy and User Guide for Network Security and Privacy**	1.0	All users

originating from your device is detected, the system administrator may suspend your connection to APU-Net without warning and deny you access to the system until security countermeasures are complete.

Prohibition of Inappropriate Use of APU-Net

You are prohibited from using APU-Net to illegally access other systems.

You may not use APU-Net to engage in illegal activity or in ways that violate the university's regulations.

Reporting Obligations

All users are asked report any security issues they may find on any of the APU systems to the Information Systems Office. In the event that a potential security flaw is detected on a system, to protect your personal data, please do not use that system until the Information Systems Office completes its review.

Regular Security Checks

Please be aware that the Information Systems Office conducts regular security checks of the information system and network.

Protection of Privacy

User files and user information must be carefully protected as forms of personal information. Attempting to access another person's protected files or data is considered a severe security breach and may be subject to disciplinary action.

Responsible Use

The APU-Net system exists to assist students, faculty and staff in their day-to-day studies, teaching, research and work. Using more system resources than you require by storing a large number of data files on the server or otherwise intentionally interfering with the normal operation of systems and networks is prohibited. In addition, please do not use APU-Net to play online games.

Prohibition of Commercial Use

APU-Net cannot be used for commercial purposes or economic gain unless permitted by the university. This includes developing software, writing text or creating media for commercial purposes or preparing advertising and/or presentations for said goods or services.

Violation of This Guide

If you violate any of the rules in this guide, access to your user account and the network may be suspended immediately without warning. In some cases, you may also lose future APU-Net privileges. For serious violations, disciplinary action will be decided after an investigation and deliberation by the

APU-Net Guide		Ver	Operating System
APU Information Systems **Policy and User Guide for Network Security and Privacy**		1.0	All users

Last updated: 2014/9/30

relevant university committee. When the misuse of APU-Net is found to be criminal in nature, students may face suspension or involuntary withdrawal, and faculty and staff may face suspension or severance. Criminal prosecution may also be pursued.

【**Contact Information**】

Please contact the Information Systems Office with any questions or comments.

Information Systems Office

Location: Building D, 3rd Floor　　Hours: Mon-Fri, 10:00-16:30

Email: system@apu.ac.jp