

# CIS Computing Guide

## Introduction

In 1988, a college student—the infamous “RTM”—wrote a self-replicating computer program. The program quickly spread across the country quicker than had ever been seen before, bringing powerful mainframe computing resources at universities, scientific research labs, and military installations across the country to a grinding halt. Since then, the title of “fastest spreading” or “most damaging” virus or worm has shifted several times, but the threat of damage persists.

The Internet was built on trust and a spirit of collaboration. It was a friendly, relatively open network centered on research, communication, and the sharing of information. Cold War politics, organized crime, and criminal mischief turned computer hacking into a high-stakes attack on this spirit of openness. A small community where front doors were seldom locked turned into a global digital metropolis where deadbolts became mandatory.

Today, YOU, as a user, are being given the keys to this community. It is a position of trust and responsibility. RIT has world-class computing resources connected to both the commercial Internet and a wide-area New York State computing grid.

Thousands of gigabytes of personal information, graduate theses, undergraduate projects, scientific research, course materials, financial records, and U.S. Government data reside on our networks.

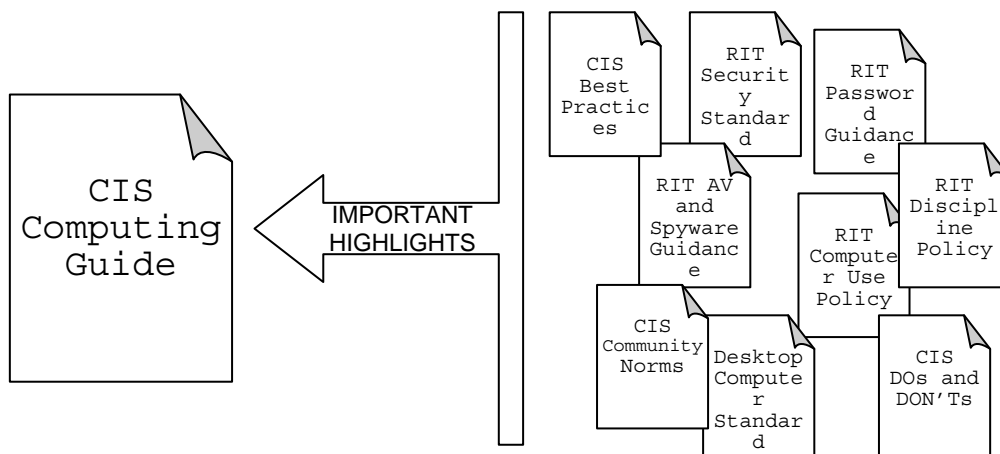
ONE user can bring it all down. There are over 10,000 authorized users at RIT, and just one can put this data, the computers on which they reside, and the networks to which they are connected at risk of damage or destruction. Safe and secure computing is everyone’s responsibility.

---

## Purpose

This guide is a quick reference and summary of computing policies in the Center for Imaging Science.

This guide does not replace RIT's computer usage guidelines



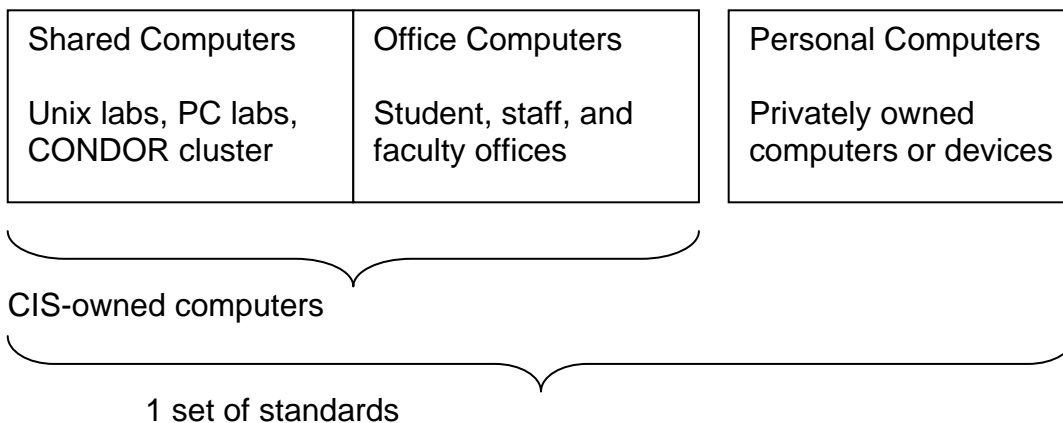
## Contents

1. Types of Resources .....	3
2. Safety and Security .....	3
3. Courteous Computer Use.....	4
4. Legal and Acceptable Use .....	6
5. Consequences .....	6
6. Emergency! .....	7
7. References.....	9

## Types of Resources

This guide covers all computers that use CIS' and RIT's network. CIS-owned computers include *shared* and *office* machines.

Privately-owned computers must also comply as a condition of being allowed access to the network.



## Safety and Security

Rules for Safer Computing:

- Each computer should only have one administrator account
- The pre-installed admin account should be disabled
- A new Admin account named cisadmin or dirsadmin should be used
- Use a limited-privilege\* account for day-to-day activity
- Install software patches and OS updates as they become available
- Use anti-virus software with current definitions
- Use anti-spyware software
- Use firewall software. Most operating systems today come with a built-in firewall.
- Do not share account information (Username or password)
- Do not open unsolicited email attachments

*\*Limited-Privilege accounts are accounts that do not have access to make changes to the system.*

## **Physical Security**

One unfortunate person left his office door open while he visited a colleague one door down. He was there for only about 5 minutes, and he didn't notice anyone enter his office. When he returned, his laptop had been stolen.

- Lock your office. If you are going to be out, lock the door
- Lock your workstation when you step away from it
- DO NOT write passwords down
- DO NOT prop open the doors to the computer labs
- DO NOT let strangers into the computer labs

## **Cryptographic Security**

Your password is the most important piece of information you own. You should not share your password with anyone.

---

---

## Courteous Computer Use

Responsible and courteous sharing on your part benefits the center's educational and research mission. Please follow these simple rules:

### Monopolizing computers or CPU time

- DO NOT lock a shared computer and walk away for an extended period of time
- DO NOT store large quantities of data—either multi-gigabyte data or non-school related files like .mp3 files—in your UNIX home directory
  - If you must, however, save it in ~/nobackup
- DO NOT run jobs on someone else's office computer.
  - You can try running the job in NICE mode, but if the owner complains your process will be killed – no questions asked.
- Learn which computers are open and shared for anyone's use.
- Run batch jobs or long programs in NICE mode.
  - Any DIRSIG job must be made NICE
  - Large MODTRAN, IDL, etc. batch jobs should also be made NICE.
- Use CONDOR to run large batch jobs. It will automatically prioritize itself properly.
- Leave your office computer on overnight. The center's backup software runs at night.

### E-mail account guidance

- You are responsible for reading e-mail to both addresses
  - E-mail is an official method of communication at RIT
  - Campus-wide announcements are sent to the RIT address
  - Center-wide announcements are sent to the CIS address
- CIS webmail is available at <http://www.cis.rit.edu/webmail>
- CIS e-mail server settings are as follows:
  - smtp server (outgoing) is mail.cis.rit.edu
  - imap server (incoming) is mail.cis.rit.edu
- If you have any questions e-mail [help@cis.rit.edu](mailto:help@cis.rit.edu)

### Care and Use

- There is no food or drink allowed in the computer labs
  - If you are discovered with food or drinks
-

## Legal and acceptable use

Our computers should not be used for any illegal activities. Some types of activities are very high-visibility. In some cases, state and federal law requires RIT to report incidents to other agencies. The following activities may result in loss of computer account

- Download or distribute copyright material (songs, movies, games, or television shows. File sharing is illegal, and copyright owners have the legal right to assert their claims.
  - RIT will bend over backwards to make sure your legal rights are being respected, but...
  - RIT cannot (and will not) shield you from the law
- Online gambling
- Pyramid money-making scams
- Exploitation of minors
- Fraud or theft
- Hacking, cracking, or any other attempt to gain unauthorized access to a computer system or data

## Consequences

Violation of the standards listed here will result in your account being frozen temporarily.

Deactivating your account is not punitive. Rather, it limits the potential damage to the system until it is safe to reactivate your account.

---

## **Illegal activity**

This is very important. There are warnings when it comes to illegal activity. If you break the law you can expect to be subject to civil and/or criminal penalties. In addition, you risk suspension, expulsion, or dismissal from RIT.

## **Intentional policy violation**

If you intentionally violate the RIT Computer Code of Conduct, you will be subject to the university's disciplinary process.

### **STUDENTS:**

RIT has a disciplinary process in place for students, and the penalties range from counseling and community service-type activities to suspension, expulsion, and fines.

### **STAFF and FACULTY:**

Staff and faculty are responsible to the Director of the Center for Imaging Science for incidents involving willful misconduct.

## **Unintentional violations**

The computer admin staff will handle the problem at the lowest level possible. The situation will be rectified, and the parties involved will be retrained so as to avoid repeating the mistake.

For example, if you accidentally infect your computer, have your password cracked, or facilitate a compromise, you will be instructed on preventing a recurrence of the problem.

## **Emergency!**

If you discover or suspect one of the following:

- Virus, worm, or macro virus on any computer (personal or CIS)
  - Spyware or adware on a CIS machine
  - Unauthorized account access
-

- password was changed
- files were moved, changed, or deleted
- strange e-mails in your outbox
- an unusual number of files or files of unusual size

Take the following steps:

- Report the incident to the computer administration staff, both for CIS computer and personal computers.
  - Jim Bodie
    - Location: 76-2144
    - Office: (585) 475-6160
    - [bodie@cis.rit.edu](mailto:bodie@cis.rit.edu)
  - Brett Matzke
    - Location: 76-2140
    - Office: (585) 475-5977
    - [matzke@cis.rit.edu](mailto:matzke@cis.rit.edu)
- CIS computers
  - Do not disconnect from the network
  - Do not shut down
- Personal computer
  - Disconnect from the network
  - Attempt to clean the computer and/or determine the extent of the damage

## **Not Quite an Emergency**

For other issues requiring assistance, you are always welcome to send an e-mail message to [help@cis.rit.edu](mailto:help@cis.rit.edu)

---

## References

You are responsible for adhering to the RIT Computer Acceptable Use policy. Please read and review the document.

RIT Code of Conduct for Computer and Network Use

<http://www.rit.edu/computerconduct/>

ITS, Information and Technology Services, provides several helpful websites.

ITS main site

<http://www.rit.edu/its/>

Security and virus protection

<http://www.rit.edu/its/services/security/>

Antivirus software

<https://start.rit.edu/virus.php>

New student information

[http://www.rit.edu/its/help/new\\_at\\_rit.html](http://www.rit.edu/its/help/new_at_rit.html)

Personal computer security checklist

<http://www.rit.edu/its/services/security/SecCheckLong.pdf>

RIT Information Security Standards

<http://security.rit.edu/standards/index.html>

---

# CIS Password Information and Change Instructions

## Rules for your CIS password:

- It needs to be greater than 6 characters
- Preferably 8 characters, it can be longer than 8, but only the first 8 are used (characters past the first 8 characters will be ignored)
- It needs to be a mix of random upper and lower case letters
- It needs to have a number or a special character in the middle of it. Preceding and post numbers are automatically taken into account in all password crackers.
- It needs to NOT have common numerical substitutions for alphabetical characters. These are very easy to crack. For example:
  - Ch33s3 is just as easy to crack as cheese.
- A good way to choose a password is to take a phrase like "Have a nice day" and take some letters from each word and put a number in the middle of it somewhere. For Example:
  - "Have A Nice Day" would be  
HaA6NiDa
- We do password crack every quarter
- If we crack your password we will disable your account. If we can get into your account, than someone else is able to get into your account
  - You will need to contact us to have it reactivated, in person
- Do not share your password with anyone
- Do not use the same password for your accounts

## To change your CIS password:

Please change your password every 6 months

Login to any of the UNIX machines and at the prompt type:

```
passwd
```

It may prompt you for your old password, if it does type in your old password and hit return.

It will prompt you for a new password.

Type in a password according to the following rules

```
hit return
```

```
confirm your password
```

```
hit return
```

It should then tell you that you password has been successfully changed.

## Acknowledgement of Responsibility and Expectations for CIS Computer Users

I have (will) read the CIS Computing Guide and understand that I am responsible for becoming familiar with the contents.

I understand the damage possible if a malicious person(s) or program(s) gain access to protected data.

I will not use CIS or RIT computers and networks for illegal purposes

I understand the minimum standards of safe computing, including strong passwords, physical security, up-to-date software, and use of anti-virus software

I will respect the community norms to ensure fair and equal access to the computing resources

I know who to contact to report an incident

I will take responsibility for my actions as an individual in whom trust has been placed by being granted computer access

Name: \_\_\_\_\_

RIT and CIS username: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

CIS Admin Signature: \_\_\_\_\_

PLEASE INDICATE TYPE OF ACCOUNT:

FACULTY    MASTERS                      PHD                      STAFF                      UGRAD                      OTHER

## Appendix B – CIS Responsible Computing Acknowledgment