Journal of Information Technology Teaching Cases (2015) 5, 102–112

palgrave-journals.com/jittc/

Teaching Case

Snowfall and a stolen laptop

Mark-David J McLaughlin[1,2], Sean Hansen[3], W Alec Cram[1], Janis L Gogan[1]

[1]Bentley University, Waltham, USA;
[2]Cisco Systems, San Jose, USA;
[3]Rochester Institute of Technology, Rochester, USA

Correspondence:
W A Cram, Department of Information and Process Management, Bentley University, 175 Forest Street, Waltham, MA 02452, USA.
Tel: +781 891 2811;
Fax: +781 891 2949;
E-mail: wcram@bentley.edu

Abstract

The E. Phillip Saunders College of Business (COB) Dean at Rochester Institute of Technology (RIT) discovers that his RIT-issued laptop has been stolen from his home. He notifies Dave Ballard, a member of the College of Business IT staff. Ballard, still acutely aware of two recent incidents in which laptops containing thousands of Social Security numbers were stolen from the RIT campus, hopes the Dean's laptop does not contain personally identifiable information. If so, the incident would need to be reported to the New York Attorney General's Office, and RIT would be required to pay for a credit monitoring service for individuals whose identity may have been compromised. The case provides an opportunity for students to examine processes that should be triggered when an information security incident occurs. The case describes incident response processes that were triggered at RIT and technologies that were used or could have been used by COB IT staff to track the laptop and protect its contents. In discussing the case, students can consider how the theft of a computing device exposes an organization to risks of inadvertent disclosure of information in different categories (such as private, confidential, internal, or public), and students can derive useful guidelines for effective information security incident response.
Journal of Information Technology Teaching Cases (2015) **5,** 102–112. doi:10.1057/jittc.2015.12
Keywords: information security; incident response; risk management; IT governance

Snow falling on Rochester

The vanity plates on the Lexus pulling up to the curb at Rochester New York International Airport in February might have seemed cryptic to a casual onlooker: EPS COB. The plates' acronym stood for E. Phillip Saunders College of Business, one of eight colleges of the Rochester Institute of Technology (RIT). In the driver's seat was the EPS COB Dean. He said goodbye to his wife, who would board a US Airways flight to Boston, where she worked.

Their home sat on a corner lot in a quiet residential Rochester neighborhood. The Dean was grateful that his snow tires retained their grip; it had again been snowing all day. Driving down Villanova Street, he clicked the remote control to raise the garage door and pulled into his driveway. The snow looked to be four or five inches deep. With his jacket and gloves already on and the snow tapering off, this was as good a time as any to get a little exercise, so he grabbed a shovel from the garage wall and set to work. It was light, fluffy snow and he completed the job in 10 or 15 min. He walked around to the front of the house (facing Carleton Road) to shovel the front steps and walk. A few minutes later, after depositing the shovel in the garage, he headed into the house through the back door, wiping his snowy boots on the doormat.

And that's when he noticed a trail of wet boot prints. 'What the …?' At first he could not make sense of what he saw, but he soon realized those were not his wet boot prints; someone had been in his house! He stepped into the kitchen and through to the den, where he had planned to spend the evening answering emails and reviewing some materials in preparation for several upcoming meetings. The intruder's trail led through the den and into the front hall. He felt a cold wind blowing through the front door – why was it open? Then he felt another chill: from the sudden realization that his laptop, which he'd left on the couch in the den before taking his wife to the airport, was no longer there. After shutting and locking the front door, he raced through the house to verify that the laptop was not in another room. Nothing else seemed amiss, but the laptop was definitely gone. Its power cord dangled from the wall.

The Saunders College Dean realized he'd better call the police – and Dave Ballard.

Urgent: laptop stolen

Dave Ballard, Network Administrator at the Saunders College of Business, was relaxing at home on a typically snowy Sunday in a suburb of Rochester when he noticed a new email from the Dean, with an ominous subject line: *URGENT: Laptop Stolen*.

'Oh, no,' he thought. 'Not again.' Two incidents in recent memory had also involved stolen laptops at RIT (although, thankfully, not at the College of Business). Personally identifiable information (PII) was stored in various files on those laptops, exposing many people to a risk of identity theft. New York law required that incidents involving such risk had to be disclosed to the State Attorney General's Office. Since it had not been possible to verify whether PII had or had not been compromised, it became necessary for RIT to offer a large number of student applicants and current students free access to an expensive credit monitoring service (when personal information is compromised in a data breach, a credit monitoring service gives victims copies of their credit reports, and monitors credit activity – such as inquiries necessary to open a new credit card account on a regular basis for a period of time. Most credit monitoring services also provide identity theft insurance covering costs associated with an incident, and professional assistance to help resolve issues that might arise from identity theft). RIT's Chief Financial Officer, highly displeased with the unexpected credit monitoring expenditures (Appendix A and B) had tasked RIT's central IT office and each College IT unit to improve the security of RIT-owned devices, data, and intellectual property stored on them.

RIT and the saunders college of business

RIT was one of the largest private universities in the United States, with 15,000+ undergraduate students, about 3000 graduate students, and a curriculum that emphasized career-oriented experiential learning. RIT's cooperative education program, in partnership with more than 2000 employers, placed students in 5000 or more co-op assignments each year. The Institute's 1000+ full-time faculty, nearly 500 adjunct faculty, and more than 2200 staff were distributed across eight colleges:

- College of Applied Science and Technology.
- E. Philip Saunders College of Business.
- Golisano College of Computing and Information Sciences.
- Kate Gleason College of Engineering.
- College of Imaging Arts and Sciences.
- College of Liberal Arts.
- National Technical Institute for the Deaf.
- College of Science.

The Saunders College had a full-time faculty of 50, about 800 undergraduates, and about 350 graduate students. Dave Ballard started working at RIT 11 years ago, while completing his undergraduate degree in Information Technology (he also earned an MS in IT degree from RIT). He had seen a few deans come and go from the College of Business. The current Dean, a native of India, had moved to the United States after completing undergraduate studies in electrical engineering at the prestigious Indian Institute of Technology. After earning his Ph.D., The Dean worked in industry for several years – including a stint as Director of Business Systems at a large company – before becoming a business professor whose research focused on operations and quality management. While being a professor, he also founded a small software firm.

The Dean had helped the faculty to revise the COB vision and mission, based on extensive conversations with faculty, business leaders, and the broader RIT community. A key concern was that Rochester's economic growth had been stagnant as a result of over-reliance for years on the fortunes of companies that once drove the local economy: Bausch and Lomb, Eastman Kodak, and Xerox. Kodak in particular had failed to successfully transition to products and services based on digital technologies. Xerox had shifted some operations away from Rochester, and Bausch and Lomb had also experienced challenges. The result: traumatic layoffs and few new jobs. The Dean wanted the Saunders College to play a role in revitalizing Rochester and the surrounding region. He argued for a business curriculum and research portfolio that would take full advantage of RIT's strengths in science, technology, and design, by emphasizing the entrepreneurial and managerial aspects of technology-based innovation. The COB Vision, endorsed by the faculty, was:

> The Saunders College of Business wants to be the gateway to the technology strengths of the Institute for building innovative commercial enterprises.

The COB Mission stated:

> The Saunders College of Business and RIT deliver experienced-based managerially relevant education dealing with the commercialization of technology and the strategic and innovative uses of technology to create a distinctive competitive edge…

Saunders faculty were hard at work developing new courses, revising existing ones, and experimenting with instructional technologies and social media to help achieve their new vision. With the curriculum effort well underway, the Dean was focused on strengthening the existing faculty's research capabilities, hiring new faculty with strong backgrounds at the intersection of technology and business, improving student retention, reaching out to alumni, strengthening ties with influential business leaders, and fund raising. His monthly *Rochester Business Journal* columns on building an innovation economy generated positive buzz and complemented RIT President William Destler's message that RIT was 'The Innovation University.'

IT governance and structure at RIT

The Saunders College of Business was one of three RIT colleges with their own dedicated IT support office; the other five colleges relied on the university's Information & Technology Services (ITS) business unit for technical support services to students, faculty, and staff. ITS managed RIT user accounts and also supported the security software on RIT laptops and assisted end users with issues related to computer hardware, software, and networking. After a security incident ITS would help users reset their university account passwords and configure replacement devices. ITS was directed by RIT's Chief Information Officer, who reported to the Treasurer and Senior Vice President of Finance & Administration (Appendix C). Although the Saunders College IT support group did not report to ITS, it did rely on ITS for infrastructural support (e.g., networking and telecommunications) and some data center services.

Another Institute-wide business unit, the Information Security Office (ISO), was responsible for publishing information security alerts and advisories, managing security vulnerabilities in the RIT network, performing forensics after security incidents, and maintaining (and enforcing) university wide security policies and standards. ISO was directed by the Institute's Information Security Officer, within the Global Risk Management Services unit – a separate arm of Finance & Administration from ITS. In the wake of earlier information breaches, ISO spearheaded a Private Information Management Initiative, which required faculty and staff to regularly scan their computing devices for private information (e.g., Social Security numbers, credit card numbers, and security codes) and to remove information which could identify an individual. New York State defined *private information* (PI) as:

> Any personal information concerning a natural person combined with one or more of the following data elements: Social Security number (SSN), driver's license number, account number, or credit or debit card number in combination with any required security code. These combinations of information are often used in identity theft.

New York's Breach and Notification Act required that RIT notify affected individuals if their private information may have been compromised. Other special-purpose laws protected specific categories of information. For example, the US Family Educational Rights and Privacy Act governed access to educational records; the US Gramm Leach Bliley Act governed record-keeping and protection of student financial records (such as financial aid applications); and the US Health Insurance Portability Accountability Act (HIPAA) mandated practices for protecting individuals' medical information.

Information security was considered a critical priority at RIT. RIT's Information Security Council included the Institute's Chief Information Officer, all members of the ISO, representatives from ITS and the Global Risk Management Service unit, representatives from each college and various administrative offices such as (in alphabetical order) Academic Affairs, Academic Senate, Alumni Relations and Fundraising, Enrollment Management, Human Resources, Student Affairs, and Student Government.

Dave Ballard's response

The Dean's email was short and to the point: 'My house was broken into and my laptop stolen. Call me.' Ballard dialed the Dean's number, but could not get through, so he emailed a reply: 'Are you okay? Safety first.' An answer came a few minutes later: 'Yes, fine. I notified the Rochester police – they will be here shortly. How soon can you get me a new laptop?'

As Manager of Technical Services for the College, Nick Francesco would need to authorize assignment of a new device, but Ballard knew that would not be a problem; obviously the Dean needed a new laptop ASAP. He replied, 'Don't worry; I'll drop by your office tomorrow around 9:30 – okay? I've already enabled our asset management system to alert me if the device attempts to connect to our servers.'

Next, Ballard sent notes to Francesco and to RIT Public Safety. He sighed and turned to his wife. 'I'll head to work earlier than usual tomorrow. There are a few things to do before I see the Dean.'

The next morning Ballard located a laptop of the same model that the Dean used. In order to minimize support issues, Saunders IT Support maintained a standardized pool of laptops, refreshed on a 5-year basis. IT Support had administrative control over laptops used by faculty and staff. Although faculty and managers could apply for administrative rights on individual devices, IT Support installed and updated most programs, scanned for malware, and performed other device maintenance activities. LANDesk, an asset management application, helped maintain a record of each authorized user's configuration (e.g., specific software packages installed on each machine). Referring to LANDesk, Ballard configured the new machine to reflect the Dean's preferences.

Having configured the new device, Ballard had a few minutes to spare before meeting with the Dean – a fortunate fact, because his email to Public Safety had generated a flurry of activity. Public Safety let him know that both ISO and ITS had been notified; each office had been in contact with Ballard as well. Nick Francesco was in the loop now, too. In fact, heading up to the Dean's office at 9:30, Ballard encountered Francesco, who was also on his way there.

> 'Let's hope he didn't have student PII on there,' said Francesco.
>
> 'I hear you,' replied Ballard. 'RIT doesn't need another round of credit monitoring for hundreds of students!'

Several RIT policies and standards covered information security (Appendix D, E and F). Data was classified into four categories: private, confidential, internal, and public. As part of the information protection standard, every department was required to identify and maintain an inventory of all private, confidential, and internal data it maintained. Francesco did not know of any specific protected data on the Dean's laptop, but from years of working with end users, he commented to Dave Ballard that it was likely that the Dean did have some sensitive data on his laptop.

The Dean routinely started his day by 7:00 am, so he was anxiously waiting for them in his office. He thanked Ballard and Francesco for the laptop, which he booted up as he described what happened – driving back from the airport, shoveling snow, discovering footprints and an open door, and the sickening realization that his laptop was gone. 'It didn't occur to me to lock my doors when I'm in the yard. From now on, that is exactly what I will do.'

From previous experience, Francesco and Ballard knew that once a laptop was gone, it was unlikely to be recovered. While they waited for the new laptop to boot, Francesco asked the Dean about information that might have been on the stolen laptop. Francesco asked 'What student records did you have on your laptop?' The Dean quickly replied 'None.'

> Francesco clarified: "Until recently we used Social Security numbers to identify our students. Are you sure you didn't have any old class rosters, exams or other records on there?"
>
> The Dean took a few seconds to deeply consider what he was asked. 'No. I am not teaching this semester, and I deleted everything from previous semesters.'

> Francesco continued: 'Think about this carefully, because it has implications much bigger than you and me. What proprietary Saunders data did you have on that laptop?'
>
> The Dean replied, 'I really didn't have anything too important. It was committee notes, faculty salary information, stuff like that. It may have been confidential, but not really proprietary.'

Seeing that his new machine was up and running, the Dean welcomed the opportunity to move on. He clicked on Outlook to verify that his emails were synched with his phone – they were. Then he said, 'We can simply look to see what I had… What about my data – where is it?'

> Francesco replied, 'As you know, RIT users are responsible for their own backups.'

Noting a look of puzzlement on the Dean's face – or was it irritation? Dave Ballard interrupted, 'The Dean does have a backup system.' He added:

> I remember that when you came here, you were surprised that we don't do full backups for everyone, because your previous employer did that for all faculty. Not to worry; I'll restore your machine from the last backup.

The expression on the Dean's face again puzzled Ballard: a flash of relief, then a hand to the forehead and a muttered expletive. The Dean's backup system did not run automatically; he had to manually initiate it, at a moment when the machine wasn't needed (since it took some minutes to complete a backup). 'I'm not sure when I ran the backup last.' said the Dean. Ballard attempted to reassure him:

> When we were troubleshooting your machine before the holiday, we performed a backup; I'll restore your machine from that. You may still be missing some things, since that backup was almost two months ago, but this is better than nothing.

As they headed back to their offices Francesco asked Ballard to retrieve the serial numbers of the stolen laptop from the College of Business inventory management system. Ballard agreed to do so right away, and added:

> I already set up an alert to fire if and when that stolen machine connects to the Internet. As you know, every time one of our machines is turned on, it will attempt to reach our auditing servers. It's a long shot, but if someone turns it on and gets a network connection, we will know.
>
> 'Too bad we can't remotely wipe laptops,' noted Francesco.
>
> Yeah, although laptops aren't constantly connected to a network the way mobile phones are, so the software is not very effective; definitely not worth the price.

A few minutes later, Ballard reported the laptop's serial number to Francesco, who reported it to the Rochester police and RIT's safety office. Francesco then contacted local pawn shops, to see if anyone had attempted to sell a device with that serial number. Recalling also the Dean's statement that the thief 'went through the house so quickly, they left the power cord plugged into the wall!' Francesco called some local computer and electronic stores to see if anyone had tried to purchase a replacement power cord. No luck there. Later that day Francesco said to Ballard:

> Most likely, the thief immediately reinstalled Windows on the Dean's laptop, and by now, probably any data stored on that machine is gone. I doubt his files would be of much use to the average crook.

Meanwhile, Ballard took a close look at the most recently backed up data from the Dean's laptop. In conjunction with the ISO office, he ran a software program that, among other tasks, searched for 9-digit numeric strings (to discover if Social Security numbers or RIT student ID numbers were stored in the Dean's files), as well as 16-digit strings (possible credit card numbers). The search revealed a few 'hits,' which Francesco later reviewed with the Dean. Among the 9-digit strings were some false positives (9-digit numbers that were not personal identifiers), and a few real Social Security numbers, belonging to the Dean, his wife, and their children. 'Since those are 'all in the family,' they are your responsibility; we don't need to notify the Attorney General,' Francesco stated. The Dean explained that the 16-digit account numbers were for personal bank accounts in India. 'That's also your responsibility,' said Francesco. 'Well, I doubt a Rochester thief will try to get access to a bank in Mumbai,' replied the Dean. 'Good thing our other banking information wasn't there.'

Moving on

Over the next 3 days, the Dean tackled the daunting task of recovering what data he could. 'Events like this never come at a good time,' he grumbled. Some missing files were needed for several events scheduled that week, for which he had been preparing. The Dean was able to recover some items from attachments stored in his Sent Items folder on the central RIT email servers. Other missing files, such as budget reports containing salary details of Saunders employees, were not in his e-mail. Not a problem; he knew who could reconstruct that information for him.

Next, a search through his jacket pockets and desk drawers yielded a surprising number of flash drives containing useful files, especially PowerPoint files (the Dean gave many presentations to fellow deans, faculty, alumni, and business leaders. He usually brought a flash drive along, rather than taking his laptop to such events). He was pleasantly surprised at the amount of content he was able to recover from these sources.

Unfortunately, he was not able to recover everything. For example, the most recent draft of his *Rochester Business Journal* column had to be recreated from memory. This consumed a few more hours of time that he really did not have to spare. Taking stock of the situation late on Wednesday evening, The Dean realized that various other documents, spreadsheets and presentations that he had created since the backup in December, were also irretrievably lost.

Still, considering the many challenges of being a Dean – such as dealing with occasionally uncooperative faculty, coaxing donations out of prominent alumni, building a business case for the Saunders College budget – the Dean felt he could quickly put this particular inconvenience behind him.

In challenging times, he relied on his sense of humor and positive outlook on life. So, by Wednesday evening he was looking forward to having a pleasant dinner with an alumnus who served on his advisory board and had become a close friend. Checking his calendar ('Good thing the calendar was stored on the network and not on my machine!'), the Dean realized that soon he and his wife would host a group of honors students for their annual appreciation dinner – always an enjoyable weekend event at their Rochester home.

All's well that ends well

Dave Ballard was relieved that the ISO concluded that the Dean's stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff, and thus expensive credit monitoring (costing US$15–$20 per affected individual), would not be necessary. The Dean had commented that the theft of his laptop was 'a valuable lesson' about the importance of backups, and he thanked Dave Ballard and Nick Francesco for their efforts.

'I guess all's well that ends well,' thought Ballard.

Suggested student case preparation questions

1. Evaluate the steps that Dave Ballard and Nick Francesco took in response to the Dean's email informing them that his laptop had been stolen. Which steps were effective, and which steps needed improvement? Be prepared to justify your reasoning by articulating your own criteria for effective or ineffective incident response.
2. Consider the role of Dean of the Saunders College of Business, including his roles as a leader, spokesperson, fundraiser, and manager. In supporting the many activities the Dean performs every day, how do digital assets on his laptop help him? What specific categories of information does he keep on that machine, according to the case? What other information might he store on his laptop, given the work that he does?
3. What strengths and weaknesses do you see in the COB InfoSec controls and incident response activities? What are lessons the two main players, Dave Ballard and the Dean, learned from this episode? What other lessons should they have learned?

Acknowledgements

An early version of this teaching case was presented at the 2014 North American Case Research Association (NACRA) Conference in Austin, Texas. The authors would like to acknowledge the NACRA members, several anonymous reviewers, and the journal editor for their insightful comments and suggestions, which have greatly enhanced this case. They also wish to acknowledge Dave Ballard, Nick Francesco, and other RIT personnel for their contributions and support in the development of this case.

About the Authors

Mark-David J. McLaughlin, a Ph.D. candidate at Bentley University, earned his MBA from St. Edward's University and BS from Texas Tech University. He has held a variety of security related positions at IBM and Cisco and was the team lead of the Product Security Incident Response Team in Cisco's Security Research and Operations group.

Sean Hansen, Associate Professor of Management Information Systems at Rochester Institute of Technology, earned his Ph.D. and MBA from the Weatherhead School of Management at Case Western Reserve University. His research has been published in several scholarly journals, including *MIS Quarterly, Information Systems Journal, Communications of the ACM, Information & Organization*, and *The Information Society*.

W. Alec Cram, Assistant Professor of Information & Process Management at Bentley University, received a BComm from Queen's University and worked as an IT Audit Manager at Deloitte before completing his MSc and Ph.D. at Queen's. His research on information systems control has been published in a variety of outlets, including the *Information Systems Journal* and the *Journal of Information Systems*.

Janis L. Gogan, Professor of Information & Process Management at Bentley University, earned EdM, MBA, and DBA degrees from Harvard University. Her many teaching cases have been taught at business schools around the world, and her research on strategic IT management has been presented at conferences such as AoM, AMCIS, ECIS, HICSS ICIS, and NACRA and in more than 40 papers published in scholarly journals.

Appendix A

Excerpt from *the reporter* (RIT student-run publication)

More stolen RIT Laptops: second major student data breach. (by Alyssa Kenny)

With the aroma of turkey on the horizon tickling at their noses, approximately 1000 students were greeted over Thanksgiving break with a letter from RIT explaining that their personal information was at risk. On 17 November, 'three laptops were discovered stolen from a locked storage area' on the RIT campus, the letter stated. The laptops were said to contain personal information.

It is believed that the laptops were stolen sometime between 7 November and 14 November. It is alleged that two of the computers contained confidential student information, including some students' names, dates of birth, and social security numbers. RIT Public Safety and the Monroe County Sheriff's office are currently investigating the theft.

According to the information that RIT sent out to the affected students, the university 'is acutely aware of the need to secure sensitive data. RIT continuously reviews practices in place to protect sensitive data.' To aid in highlighting the importance of protection as well as to alleviate some of the stress the incident may have caused, RIT is providing each affected student with a free 1-year trial of Experian's Triple Alert. Triple Alert is a credit-monitoring product, which will monitor the student's credit reports at Experian, Equifax, TransUnion, the three main national credit reporting companies. RIT hopes that the affected students will take advantage of this opportunity to have the product identify potentially fraudulent use of their information and ensure their protection from identity theft.

According to a Federal Trade Commission survey, identity theft is the fastest growing crime in America. Last year alone, 9.9 million victims were reported.

Electronics are a hot commodity at RIT. At a school as electronically dependent and technologically renowned as RIT, it is imperative for students to protect their electronics and identity from theft and hacking, and for everyone to guard against potential laptop theft.

Appendix B

Excerpt from *University News* (RIT News and Public Relations Division)

College of design and architecture STOLEN LAPTOP

RIT recently discovered that personal information was on a laptop computer stolen from the National Technical Institute for the Deaf on 25 August. The information included names, dates of birth, and Social Security numbers.

Note: Letters were mailed to those affected. This information security alert does NOT affect the entire RIT community, but a specific population. This includes about 12,700 individuals who have applied to enroll at the National Technical Institute for the Deaf (dating back to 1968). Another 1100 members of the RIT community have also been impacted. Again, people affected have been notified individually.

A toll-free hotline has been established at 1-866-624-8330. You will be able to call this number through a relay service. The hotline will be available from Tuesday, 2 September, through Friday, 26 September, and you may call from 9:00 to 21:00 (Eastern Time) on weekdays, and on Saturdays from 10:00 to 16:00.

Appendix C

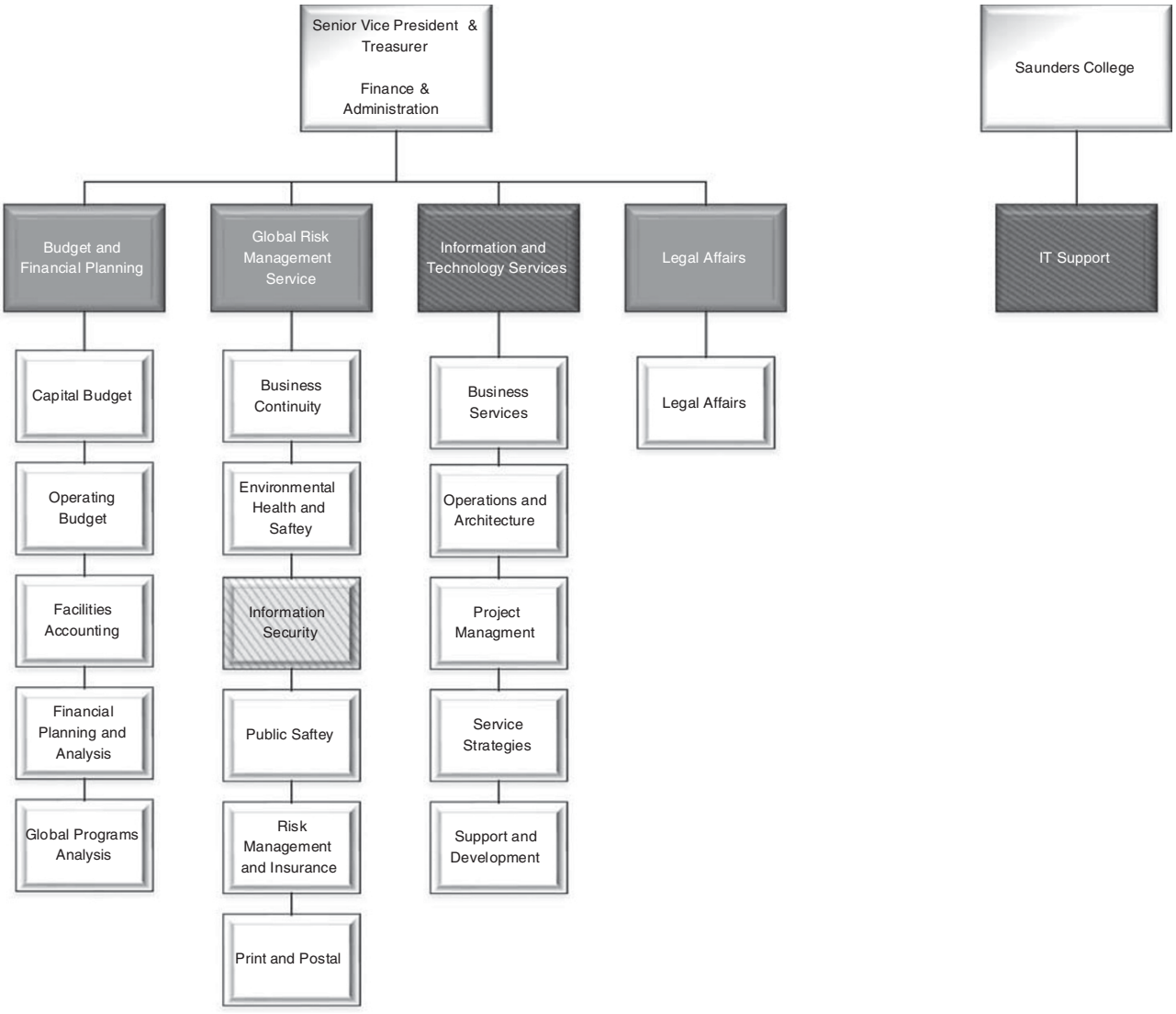

Figure C1 Partial RIT administrative organization chart.

Appendix D

RIT information security policy

The information assets of Rochester Institute of Technology (RIT) must be available to the RIT community, protected commensurate with their value, and administered in conformance with federal and state law. Reasonable measures shall be taken to protect these assets against accident or unauthorized access, disclosure, modification or destruction, as well as to reasonably assure the confidentiality, integrity, availability, and authenticity of information. Reasonable measures shall also be taken to reasonably assure availability, integrity, and utility of information systems and the supporting infrastructure in order to protect the productivity of members of the RIT community, in pursuit of the RIT mission.

Information safeguards are administrative, technical, and physical controls that support the confidentiality, integrity, availability, and authenticity of information. *Information systems and supporting infrastructure* consists of information in its analog and digital forms and the software, network, computers, tokens, and storage devices that support the use of information.

Controls depend on the system, its capabilities and expected usage, and anticipated threats against the information.

- *Preventive controls* include use of encryption, information integrity measures, security configuration, media reuse, use of antivirus, and physical protection.

- *Detective controls* include network and information access monitoring, and intrusion detection (host-based or network-based), manual or automated review of security logs.
- *Corrective controls* include recovery plans for handling isolated information safeguard failure incidents to business continuity plans.

RIT will take reasonable steps to:

1. Designate one or more individuals to identify and assess risks to non-public or business-critical information within RIT and establish a university-wide information security plan.
2. Develop, publish, maintain, and enforce standards for life-cycle protection of RIT information systems and supporting infrastructure in the areas of networking, computing, storage, human or device/application authentication, human or device/application access control, incident response, applications or information portals, electronic messaging, and encryption.
3. Develop, publish, maintain, and enforce standards for RIT workforce security related to the irresponsible use of information.
4. Provide training to authorized university users in the responsible use of information, applications, information systems, networks, and computing devices.
5. Develop, publish, maintain and enforce standards to guide RIT business associates and outsources partners in meeting RIT standards of lifecycle protection when handling RIT information or supporting RIT information systems and supporting infrastructure.
6. Encourage the exchange of information security knowledge, including threats, risks, countermeasures, controls, and best practices both within and outside the university.
7. Periodically evaluate the effectiveness of information security control in technology and process.

Appendix E

RIT acceptable use policy

Policy name: Code Of Conduct For Computer and network use (C8.2)

I. Introduction

The computing, network, and information resources of RIT are intended to support the mission of teaching, scholarly activity, and service for the University's students, faculty and staff. Appropriate use of computing and networking facilities by members of RIT's academic community should always reflect academic honesty and good judgment in the utilization of shared resources, and observe the ethical and legal guidelines of society. This document constitutes RIT's policy for the proper use of all computing and network resources.

RIT's computer and network facilities provide access to a wide variety of on and off campus resources. This privilege of access requires individual users to act in an ethical manner and as a result imposes certain responsibilities and obligations. It is the responsibility of every user to respect the rights, privacy, and intellectual property of others, and abide by all local, state, and federal laws and regulations.

This document outlines the user privileges and responsibilities as well as the guidelines and procedures for the responsible use of the RIT computer systems and networks. It is intended to allow for the proper use and management of these facilities, provide protection of users' rights, ensure reasonable access, and provide guidelines for accountability. It applies not only to RIT computers and networks, but also to computers attached to RIT's networks in any way.

II. Definitions

To avoid ambiguity, the following definitions are supplied:

A. *User* – Anyone who uses computing or network facilities.
B. *Authorized University User* – Anyone who has followed account application procedures and has been granted access to any or all of the computing or network resources of RIT for reasons consistent with the mission of the university, and consistent with this policy.
C. *University Computing Resources* – Any computing, network, or software system donated to or purchased by the University or by a grant that is resident at the University.
D. *University Network* – The network of the University comprising the physical components such as cable, switches, telecommunications equipment, wireless hubs, routers, Virtual Private Network (VPN) concentrators, dial-up access points, as well as the Internet and Internet2 connection points. The University network also has logical components such as IP addresses, directory services, routing, and connectivity to computing resources.
E. *University Network Connections* – Any computer or device using an Internet address assigned to RIT or that is connected to a physical or wireless access point is considered to be connected to the University network.
F. *Personal Computing Resources* – Personal resources such as PCs, networking equipment, and so on, which have been purchased and are owned by an Authorized University User and are connected to the University network.
G. *Special Access* – Access to resources on a system that could be used to alter the behavior of the system, or to access accounts on the system. Examples are UNIX 'root' or Windows 'Administrator.'

H. *System Owner* – The person with the authority to designate or use special access account privileges.
I. *System or Network Administrator* – The person responsible for maintaining the authentication used by the system or network, controlling authorized use, and maintaining system and network integrity and audit trails.
J. *Secure Systems* – Any hardware or software system whose use is restricted to a subset of the community of legitimate RIT users.

III. Relationship to other university policies
A. University Policies – Many issues addressed in this Code of Conduct relate to existing University policies, including (but not limited to) the University's policies on privacy, intellectual property, and prohibition of discrimination and harassment (found elsewhere in this Manual). This Code is intended to supplement and clarify the guidelines laid out in those policies as they apply to use of computer systems and electronic resources, not to supersede them.

B. Other Computer Use Policies – Campus units that operate their own computers or networks are encouraged to add, with the approval of the unit administrator, additional guidelines that supplement, but do not lessen, the intent of this policy or other University policies. In such cases, the unit administrator will inform users within the unit and will provide a copy of the unit-level policy to the Chief Information Officer and to the Information Security Officer.

IV. User privileges and responsibilities
A. Privacy – The University's 'Privacy Policy' (C7.0) recognizes that 'Individual privacy and security are highly valued by our society,' but 'must be balanced by the other community enumerated values and needs.' Within this understanding, the RIT community is assured that the privacy of such 'personal property' as 'written communications intended by their creator to be private including those transmitted or preserved in paper, electronic, or other media' will be protected, although it cannot be completely guaranteed.

The 'Privacy Policy' also recognizes that members of the RIT community have a responsibility to cooperate with authorized searches and seizures in emergencies and in circumstances of probable cause. In such instances, including those involving RIT computer and network use, the search and/or seizure of personal property or personal communications will be executed only on the authorization of an official identified in the 'Privacy Policy.' Cooperation with the search or seizure of one's personal property or personal communication does not of itself imply one's own misuse or abuse of RIT computers or network; the search or seizure may be deemed necessary because of misuse or abuse elsewhere in the RIT system or in systems to which the RIT system is connected or affiliated. For example, scanning and pattern matching of incoming or outgoing e-mail may be necessary to remove computer viruses, to locate the sources of spam, or to respond to legitimate internal or external requests for investigation. In all instances of investigation into personal computing and network use, individuals are protected to the extent possible by the provisions of the 'Privacy Policy.'

B. Freedom from Harassment – The RIT 'Policy Prohibiting Discrimination and Harassment' (C6.0) defines 'harassment' as unwelcome 'conduct, communication, or physical contact' which has the effect of either 'unreasonably interfering with' another's work, activities, or participation, or of 'creating an intimidating, hostile or abusive environment' for a RIT employee or student. Members of the RIT community are assured that electronic communications that appear to have one or more of these effects are prohibited and will be investigated. This prohibition includes all obscene, defamatory, threatening, or otherwise harassing messages.

Correspondingly, members of the RIT community have the obligation not to use the RIT computing systems and network in such a way as to be reasonably judged to produce one or another of the above effects, whether intentionally or unintentionally. Such alleged or real misuse is covered by the provisions of this Code of Conduct as well as by the 'Policy Prohibiting Discrimination and Harassment' (C6.0).

C. Intellectual Property – The RIT policy on 'Intellectual Property' (C3.0) deals in a detailed and exhaustive way with the rights of RIT employees as creators and owners of intellectual property. The privilege of creating and owning intellectual property as outlined in that policy is fully recognized by this Code of Conduct.

However, where a violation of the 'Intellectual Property Policy,' or of the intellectual property rights of creators or owners beyond the RIT campus, is alleged to have occurred through student or employee misuse of the RIT computing systems and network, such alleged misuse will be investigated and, if proved, sanctioned.

For example, RIT users must not distribute copyrighted or proprietary material without written consent of the copyright holder, nor violate US copyright or patent laws concerning computer software, documentation, or other tangible assets. Users should assume that any software or other electronic materials or media are copyright protected, unless the author(s) explicitly states otherwise.

D. Freedom of Expression – In general, all members of the RIT community–students and employees alike – enjoy freedom of expression in the normal course of their activity.

This freedom is both assured by numerous University policies and constrained by specific provisions of certain RIT policies, such as those noted herein (C3.0, C6.0, C7.0, and C10.0) as well as by specific provisions of this Code of Conduct. The constraints are, as in civil law, imposed only for the sake of the common good and the rights of individuals. Consequently, members of the RIT community have the responsibility to use RIT's electronic resources in ways that respect the rights of others and permit our common electronic resources to be equitably shared. Since free and civil discourse is at the heart of a university community, users should communicate in a manner that advances the cause of learning and mutual understanding.

RIT reserves the right to restrict or deny access to its computing resources to those whose use of them is not consonant with the mission of the university.

V. Responsible use of resources

In exchange for the privileges associated with membership in the RIT computing community, users assume the responsibility to use the community's resources in a responsible and professional manner. The following paragraphs (A–G) highlight a non-exhaustive list of specific responsibilities. Questions about the appropriateness of any use of resources should be directed to the staff of the Division of Information and Technology Services or to the systems personnel responsible for the resource in question.

A. Access to secure systems

1. *Passwords and similar authorization information* – Passwords are the primary way in which users are authenticated and allowed to use the community's computing resources. One should not disclose one's password(s) to any individual, including a faculty or staff member, unless the person is a properly authorized system administrator performing account maintenance activities for which the password is required. Similarly, one should not disclose other identifying information (e.g., PIN numbers) used to access specific system information. Authorized users are held accountable for violations of this Code of Conduct involving their accounts.
2. *Unauthorized use of resources* – One must not allow others to make use of one's account(s) or network access privileges to gain access to resources to which they would otherwise be denied.
3. *Circumventing or compromising security* – Users must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the RIT systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and the launching or knowing transmission of viruses or worms.

B. Self-Protection – Any member of the RIT community who attaches a computer to the RIT network must take measures to ensure that the computer is protected against compromise by an internal or external attack. In this context, reasonable measures include the installation and maintenance of virus detection and eradication software, care in opening e-mail message attachments, vigilance when visiting Websites and adhering to published system configuration and management standards.

C. Commercial Activity – No member of the RIT community may use a RIT computing account or any communications equipment that is owned or maintained by RIT to run a business or commercial service or to advertise for a commercial organization or endeavor. Use of RIT's computer systems and networks for the personal promotion of commercial goods or services is strictly prohibited. RIT employees who are engaged in professional consulting for-a-fee relationships may use RIT's computing and network resources to correspond with existing clients, but not to advertise or promote their consulting practice.

D. Personal Use of RIT Resources – In general, the use of RIT's computing and network resources to promote commercially-related activities or events that have no direct relationship to RIT's mission is not permitted. Occasional personal use of these resources, for example, to promote a single fund-raising event or activity, to sell a used item within the RIT community, or to offer RIT colleagues the opportunity to rent a house may be permitted at the tacit discretion of the Chief Information Officer.

E. Communication with Government Officials – E-mail communications with government officials must abide by RIT's guidelines for political activities as outlined in policy C10.0. Individuals wishing to address a legislative issue on behalf of the university should consult with the Office of Government and Community Relations before sending such communications using RIT's network.

F. Harmful Activities – One must not use one's privileges as a member of the RIT computing community to cause harm to any individual or to harm any software or hardware system, whether internal or external to RIT. Examples of harmful activities, in addition to those noted elsewhere in this Code, include:

1. Intentional damage
    - Disabling others' computers
    - Compromising security
    - Disabling or corrupting software systems
    - Destroying, altering, or compromising data integrity (e.g., student records, personnel information, etc.)
2. E-mail spamming
3. Threatening or intimidating e-mail, newsgroup postings, or web sites.
4. Denial of service attacks (e.g., making it difficult or impossible for others to use the network).

G. Illegal Activities – For the protection of the RIT computing community as a whole, it is imperative that all members refrain from any conduct that is illegal. Illegal activities that are prohibited include (but are not limited to):

1. Copyright infringement, including publishing copyrighted material such as papers, software, music, musical scores, movies, and artistic works. It is irrelevant whether or not any profit is made from such distribution; the mere fact of providing uncontrolled access to such material is illegal.
2. Divulging information that is confidential or proprietary information.
3. Misrepresentation of one's identity to gain access to systems, software, or other services to which one does not have authorized access.

Appendix F

RIT information classifications

Private – a classification for information that is confidential which could be used for identity theft and has additional requirements associated with its protection. Private information includes:

- Social Security Numbers (SSNs), Taxpayer Identification Number (TIN), or other national identification number
- Driver's license numbers
- Financial account information (bank account numbers (including checks), credit or debit card numbers, account numbers)

Confidential – a classification for information that is restricted on a need to know basis, that, because of legal, contractual, ethical, or other constraints, may not be accessed or communicated without specific authorization. Confidential information includes:

- Educational records governed by the Family Educational Rights & Privacy Act *(FERPA)* that are not defined as directory information
- University Identification Numbers (UIDs)
- Employee and student health information as defined by Health Insurance Portability and Accountability Act *(HIPAA)*
- Alumni and donor information
- Employee personnel records
- Employee personal information including: home address and telephone number; personal e-mail addresses, usernames, or passwords; and parent's surname before marriage
- Management information, including communications or records of the Board of Trustees and senior administrators, designated as confidential
- Faculty research or writing before publication or during the intellectual property protection process.
- Third party information that RIT has agreed to hold confidential under a contract

Internal – a classification for information restricted to RIT faculty, staff, students, alumni, contractors, volunteers, and business associates for the conduct of University business. Examples include online building floor plans, specific library collections, etc.

Public – a classification for information that may be accessed or communicated by anyone without restriction.