Procurement Card Best Practices and the Policies for Selected Discretionary Expenditures

**Procurement Card Best Practices**

RIT employees may apply for a procurement card (P-card) to purchase RIT business-related products; applications are subject to approval by the Procurement Services Office (PSO). The Procurement Card Guide, developed by RIT’s Controller’s Office, contains detailed parameters for using P-cards. Cardholders are expected to comply with RIT procurement policies when making purchases. The P-card is intended for official RIT business-use only and may not be used for personal purchases. All business related P-card purchases must be (1) reasonable and necessary, (2) authorized by appropriate individuals with budget authority, (3) consistent with RIT’s mission, and (4) compliant with restrictions.

The typical individual transaction limit is $1,500 and the suggested monthly credit limit is $2,500, with any exceptions requiring approval by the PSO. A cardholder is expected to check the card’s available balance and plan accordingly for the purchases required during each month.

A purchase made with an RIT P-card should have a clearly defined business purpose ("who," "what," and "why") and original supporting documentation (i.e., receipts/invoices, list of all attendees at business meals, proof of receipt). Purchases made with the P-card should not include sales tax, as RIT has been granted an exemption from NY state sales tax. The cardholder should use the PNC Active Pay system (Active Pay) to document the business purpose of the purchase and also designate the correct account combination. Other information can be included on the original supporting documentation.

Expenses incurred via an individual P-card must be properly reviewed and approved by an employee who is at least one-level of management above the cardholder and has signature authority to approve financial transactions. For departmental P-cards, a second approver, who must be one-level above the cardholder's supervisor and has signatory authority for the department, must also review the expenses and supporting documentation. The PNC Procurement Card Monthly Certification Form must be signed, dated, and submitted in accordance with the RIT Procurement Card Guide.


**Policies for Selected Discretionary Expenditures (a.k.a. the Discretionary Spending Policy)**

Through our audits of the P-card program, we note occasional instances of non-compliance with RIT’s business-related discretionary spending policy in the areas of meals/hospitality and gifts for employees. A few general reminders about the discretionary spending policy and allowable expenditures in these areas follow:

Business meals fall under RIT’s Policies for Selected Discretionary Expenditures. Typically, allowable business meals include (1) those taken with business associates and professional colleagues outside of RIT, prospective students or donors, and job applicants to discuss RIT business-related items; (2) those taken at on-campus dining establishments for two or more RIT employees scheduled during lunch or dinner time, when no other time was available for the meeting and where RIT business is discussed; and (3) those incurred when RIT faculty, staff, or students travel on RIT business. Note, however, that the P-card should be used for local off-campus hospitality meals only; it should not be used while traveling.

Alcohol purchases, although generally unallowable, may be allowed in situations where business-related activities occur that relate to the mission of the University and involve individuals external to the RIT community, as well as at University-sponsored events when approved by a division Vice President. It is important to ensure that these costs are charged to the proper object code. A cardholder needs to indicate on the original supporting documentation if alcohol was purchased on the P-card; the cost for the alcohol must be allocated to object code 79050 – Government Unallowable Charges. The change in the object code can be easily completed in Active Pay prior to when the transactions are imported and posted to the general ledger, which occurs at the end of the month. If the object code change is not completed prior to that time, a journal entry will be required.

Although personal meals (e.g., birthday lunches, secretary’s day lunches) are not allowed, expenses reasonable in scope are allowed for holiday parties and summer picnics, provided they include all employees within the department. Refer to the Policies for Selected Discretionary Expenditures for the current upper limits for such events, and note that these activities must be authorized by the responsible Dean or Vice President.

While holiday or personal (e.g., birthday, boss’s day) gifts to employees are not considered valid business-related expenditures, gifts made to employees upon retirement from RIT under a general guideline of $10/year of service (with a maximum of $400 including delivery, S&H, etc.) are allowable. Gifts to active and potential donors must be properly reviewed and approved by the divisional Development/Alumni Relations representative. An RIT Gifts Given Form, available on the Controller’s website, must be completed for all gifts.

If you are unsure whether a purchase you are about to make with your P-card complies with RIT’s Procurement Card Guide or the Policies for Selected Discretionary Expenditures, contact the Controller’s Office for guidance. Ultimately, it is each cardholder’s and the approvers’ responsibility to ensure they are aware of all of RIT’s policies regarding the proper use of an RIT-issued P-card.

~~ Contributed by Alice Jatsenti
Associate Internal Auditor
Institute Audit, Compliance & Advisement
Inform RIT is a recurring column provided by the RIT Information Security Office. The column highlights current issues and initiatives that impact the RIT community. In this issue, we’ll talk about Zero-Day exploits and why they should matter to you.

Zero-Day Exploits and Why They Should Matter to You

There’s a lot of jargon thrown around in information security. Some of it’s important for the average computer user to know; much of it is not. One term you may have heard of that is important for you to know is “Zero-Day” exploits.

Zero-Day exploits take advantage of vulnerabilities in software (or hardware) for which the software (or hardware) vendor has not yet created a patch (or fix) for the problem. Of greater concern to us, is that anti-virus software often does not detect these exploits. In the last week of January, there were at least two malicious attachments containing zero-day exploits that reached RIT end user email accounts.

The phishing emails below contained attachments with zero-day exploits.

The January Attacks

The first attack was a fake Adobe Creative Suite invoice with a malicious file attached, invoice.doc. At the time the email was received, McAfee (and most other anti-virus programs) did not flag the attachment as infected, nor did the Brightmail spam-filtering mail appliance detect it.

The second attack posed as a response to a job posting with the subject line, Quick Question. Here’s the text:

What’s Up?
I was visiting your website on 1/29/2016 and I’m very interested.
I’m currently looking for work either full time or as an intern to get experience in the field.
Please review my Resume and let me know what you think.

Thank you for your recommendation,
--
Lavera Frias

The attachment, resume.rtf, was malicious, but again, on the day it arrived McAfee failed to detect it. (After being updated, McAfee did detect it.)

One security vendor, VirusTotal, provides a free online malware scanner to which you can submit suspicious files for analysis. VirusTotal also provides a scorecard showing which anti-virus programs identified the file as malware and the file’s detection ratio. (The detection ratio is the number of anti-virus programs identifying the file as malware over the total set of anti-virus programs measured by VirusTotal.) Here’s the virustotal for resume.rtf. You’ll see that at the time of submission, only 11 of 54 anti-virus programs were detecting it. (You’ll also see that anti-virus programs do not use the same detection names.)

(continued on p. 4)
**Limitations of anti-virus software and filtering**

As an end user, I would have two questions: 1) Why didn’t my anti-virus program or the spam filter identify and stop the malware, and 2) What do I do to protect myself if I can’t rely on anti-virus?

**Why didn’t either my anti-virus or the spam filter identify and stop the malware?**

We talked in a previous *Inform RIT* (Spring 2015) about the limitations of anti-virus. Here’s an excerpt from that column.

> Most anti-virus products score well against known samples. However, new malware variants are created hourly, and your anti-virus may or may not be good at detecting unknown malware. Anti-virus relies on two types of detection, signatures (also known as DAT files) of known malware and heuristic detection (behavioral analysis) of unknown malware. Not surprisingly, anti-virus doesn’t do as well against unknown malware threats as it does against known threats.

Because these zero-day attacks are new malware variants, there’s no detection signature available for the anti-virus programs, and they must rely on heuristic detection, which is not as reliable.

The mail filter is very good at detecting and preventing mass attacks (many copies of the same email) from reaching RIT mailboxes. These attacks came through individually or in small groups. If the mail filters were tuned to be more aggressive, they would block legitimate email from reaching us.

**What do I do to protect myself and others if I can’t rely on anti-virus or mail filters?**

Do you remember how we always advise you not to open unexpected attachments? The two phishing emails with malicious attachments provide great examples of why you should follow our recommendation. You CANNOT rely on technical solutions, such as anti-virus, to provide you with complete protection. You MUST follow good security practices when processing your email. We are targeted by cyber criminals. They WILL try to trick us into making mistakes.

Report phishing attempts by creating a new message to spam@rit.edu and dragging the suspected phishing message into the new message.

For more information, visit the RIT Information Security website ([www.rit.edu/security](http://www.rit.edu/security)) and register and attend a Digital Self Defense 101 class through the RIT Center for Professional Development.

If you’d like us to present a DSD101 class or discussion around current issues to your department, please contact me at infosec@rit.edu!

~~ Contributed by Ben Woelk
Program Manager
RIT Information Security Office

---

**What about ethics in the workplace?**

Learn about the [RIT Ethics and Compliance Hotline](#)
Internal Controls and Fraud in the Workplace

During the 2.5 hour Internal Controls and Fraud in the Workplace class, the importance of components of, and the responsibility for establishing and maintaining effective internal controls are discussed. Various examples of what can happen when controls are non-existent or break down (i.e., fraud) are shared throughout the class. The session is required to receive the RIT Accounting Practices, Procedures and Protocol Certificate of Completion. However, anyone interested in learning about internal controls and fraud prevention is welcome to attend.

To learn more about these important topics, sign up for a session at the CPD website.

Unit Level Risk Assessment—How to Advance Your Organization’s Agility

The first step towards successfully managing risks is to implement an effective risk assessment methodology. Risk assessment is a systematic process for identifying and evaluating both external and internal events (risks) that could affect the achievement of objectives, positively or negatively. During this two hour class, we will discuss the key components of an effective risk assessment process and how to integrate it into the business process to provide timely and relevant risk information to management. To learn more about this offering, see the corresponding CPD webpage.

Upcoming Internal Controls & Fraud in the Workplace Training Sessions:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, April 12, 2016</td>
<td>1:30pm to 4:00pm</td>
<td>2140 Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

Upcoming Unit Level Risk Assessment—How to Advance Your Organization’s Agility Training Sessions:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday, March 23, 2016</td>
<td>2:00pm to 4:00pm</td>
<td>2140 Louise Slaughter Hall</td>
</tr>
<tr>
<td>Tuesday, August 2, 2016</td>
<td>10:00am to 12:00pm</td>
<td>2140 Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

Watch IACA’s Monday Minute video series here!

This video series focuses on opportunities for improving internal controls and increasing awareness of various university processes, policies, and protocols. If you have questions, feel free to contact anyone in the IACA office using information on our webpage.

Past topics include: Information Security Standards, Lenel Card Swipe Access Management, Conflict of Interest & Commitment Disclosures, Records Management Policy, Risk Assessment and many others.
COSO Corner

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

As explained in previous editions of the Quaestor Quarterly, the COSO Framework (internationally recognized standard against which the adequacy and effectiveness of an organization’s internal controls are evaluated) was updated in May 2013 to further define the principles underlying the five components of internal control (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring). According to the Framework, these principles are fundamental concepts that must be present and functioning in order to achieve an effective system of internal control. In addition, the Framework includes points of focus or characteristics that are examples of behaviors or processes that would be expected to be in place to demonstrate that the related principle is in fact present and functioning. This edition of the COSO Corner will summarize the seventh COSO principle which is the second principle related to the Risk Assessment component of the COSO Framework, as well as the related points of focus.

Principle 7 – The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. The related points of focus for this principle and how they are relevant to RIT operations include:

- Risk identification considers risks at various levels of the organization’s structure including the entity (RIT) and its subunits (i.e., college, division, and department level), as well as operational processes (i.e., cash handling, graduation certification, purchasing, grant administration). As risks are assessed at each level of an organization, the focus will generally shift from broader strategic risks to more detailed operational and transaction-level risks.
- Risk identification considers both internal and external factors and their impact on the achievement of objectives. Examples of internal factors include management structure, staffing levels and competency, and technology considerations; external factors would include economic outlook, regulatory requirements, and market expectations (i.e., affordability, career preparation).
- The organization implements effective risk assessment mechanisms that involve appropriate levels of management both at the overall entity (President and Provost) and subunit (Deans and Vice Presidents) levels.
- Identified risks are analyzed through a process that includes estimating the potential significance of the risk. For example, performance measures (i.e., measurable outcomes) are utilized to determine the extent to which objectives are being achieved, and normally use the same or a congruent unit of measure when considering the potential impact of a risk on the achievement of a specified objective.
- Risk assessment includes considering how identified risks should be managed and whether to accept, avoid, reduce, or share the risk. In evaluating risk response options, management should consider the significance, including both the likelihood and impact, of a risk. Resources always have constraints, and management also needs to consider the relative costs and benefits of the various risk response options.

Reference

~~ Contributed by Nancy A. Nasca
Manager
Institute Audit, Compliance & Advisement
Take the Pop Quiz Challenge! Correctly answer the question below and you will be entered in a drawing to win a prize valued at $15. One lucky winner will be chosen randomly and notified by email.

**Question:**
According to *Inform RIT*, Zero-day exploits take advantage of vulnerabilities for which a hardware/software vendor has not yet created a _____ to fix the problem.

A. Spam  
B. Patch  
C. Stitch  
D. Antibiotic

**Post your answer to our Quiz webpage at:**
https://www.rit.edu/fa/iaca/content/quiz

****************************************
Congratulations to Patricia DiPassio from International Student Services for correctly answering the Fall issue’s Pop Quiz question.
The question and the correct answer were:

According to *Inform RIT*, safe online shopping practices include:

A. Making purchases on encrypted sites only  
B. Using a secure internet connection  
C. Using a secure payment method  
D. All of the above

Correct