# SHADOW IT POLICY

By Scott Matteson • June 2017

TECH PRO RESEARCH

# Shadow IT policy

Published by Tech Pro Research
June 2017

## Credits

**Editor In Chief**
Jason Hiner

**Managing Editor**
Bill Detwiler

**Feature Editors**
Jody Gilbert
Mary Weilage

**Assistant Editor**
Amy Talbott

## Disclaimer

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Tech Pro Research
9920 Corporate Campus Dr.
Suite 1000
Louisville, KY 40223
http://techproresearch.com

Tech Pro Research is a ZDNet Web site.

## Summary

Shadow IT is a recent phenomenon whereby an organization’s employees use technology, services, or systems without knowledge of or approval from the IT department. It has arisen due to several reasons:

- Advances in cloud computing, which involve the usage of applications or sharing of data in public environments previously owned by IT
- The evolution of complex consumer technology, which has helped many lay people become familiar with how applications and processes work
- Cumbersome IT requirements and lack of flexibility in meeting user needs

Simply put, many users opt to make an end run around what they perceive as a stodgy or restrictive IT department to get their needs met in a timely fashion.

Shadow IT can help promote user productivity, self-reliance, and technological familiarity, but it can also pose serious risks to data security and corporate compliance. In addition, it can undermine the purpose of having an IT department: to ensure data protection and provide assistance to users when problems occur. A user who sets up a cloud storage service for sharing files with others may create compliance and security operational hazards that can wreak havoc if unchecked. Critical services or data may not be backed up or might be stored with inappropriate permissions (or no permissions at all), systems might not be patched or locked down, or a data breach could occur that could place the company at significant risk.

Shadow IT is up and running in many companies. Symantec’s CSO survey found that, “37 percent of respondents indicated they believe individual users or business units at their organization are frequently or occasionally deploying applications or putting data in the cloud without consulting IT. CSOs have no idea who these users are, but they know that the services are being used.”

It’s clear that shadow IT has both advantages and drawbacks and needs a well-defined structure for businesses to properly control it. It can be tempting to simply ban shadow IT across the board, but such a policy might only serve to further the concept that the IT department isn’t meeting user or company needs.

## Purpose

This policy provides guidelines for the appropriate use of shadow IT, explains the restrictions that will apply to it, and defines elements pertaining to employee and IT department responsibilities.

## Scope

This policy covers all full- and part-time employees, contract workers, consultants, interns, and temporary workers. It also applies to all company-owned equipment or material related thereto, along with any personally owned devices, applications, or accounts used for company business.

# Exceptions

There are no exceptions to this policy unless permitted in writing by the HR and IT departments, which will be responsible for reviewing the details, risks, and operational requirements involved.

# Policy details

## Allowable scenarios

Shadow IT is permitted but only for non mission-critical applications, services, or processes. Examples of permitted shadow IT that can be implemented and run by users include development or personal productivity tools, blogging, time tracking, or other elements that are not considered "production." In short, revenue-generating components, or those that would adversely affect the business if failed or unavailable, must remain under the control of the IT department.

## Employee responsibilities

Employees seeking alternative/additional technological processes should consult with the IT department to determine whether existing solutions can be applied or IT can implement these required processes for the organization. If not, employees should build a justification explaining what they need, why the alternative works for them, and how they intend to use it. They should present this justification to the IT department for review and approval. Operational requirements (who will maintain the process or processes, what level of access may be granted to users, performing support, etc.) must be scoped and documented in advance. This need not be cumbersome and could constitute a single page.

Approved shadow IT solutions (and the employees who utilize them) can follow Tech Pro Research's Information Security Policy and Cloud Data Storage Policy to ensure that appropriate standards for data management and secure practices are met. In a nutshell, no confidential or sensitive data should be stored in any shadow IT solution without proper controls and handling, such as encryption and access only by authorized personnel.

Complex passwords that change periodically should be used for any external applications/services not directly under IT control. Where possible, the IT department should set up single sign-on access to permit the secure usage of existing corporate credentials. (See the next section.)

Any passwords used for administrator access to a shadow IT solution should be centrally stored in a password management database (such as Password Safe or KeePass) to which IT has access, to ensure appropriate management.

If a shadow IT implementation no longer meets employee needs, becomes obsolete, or is to be retired, the employee(s) responsible should work with the IT department to do so.

## IT department responsibilities

The IT department should identify critical applications, services, and processes to establish them in a "no fly zone," making them off limits for shadow IT. For instance, a sample blogging or task management site is likely to be less of a security threat if compromised than a database storing private customer data in the cloud.

Existing rules, requirements, and policies regarding application and data usage should be reviewed for clarity. The goal should be to help make rules simple and easy to understand and not too restrictive, where possible.

The IT department should ensure the education of employees regarding the need for current security standards and requirements, so as to make it clear why the need for such protections exists.

The IT department should stay focused on and be familiar with the latest technological developments to help leverage new solutions for the business.

The IT department should review and respond to shadow IT requests from employers to ensure a satisfactory turnaround time and to facilitate the implementation of needed solutions.

Upon implementation of this policy, the IT department should provide a grace period for existing shadow IT deployments involving critical systems that will be placed under IT management as needed, with no repercussions to the users involved.

The IT department should promote an "open door" environment for employees to provide input into their needs. These needs should be the foundation for advice and guidance for the design and implementation of new projects and solutions.

CIO magazine recommends asking these questions when employees suggest a shadow IT solution:

- "Is there a reason why a particular solution is inappropriate for the company?"
- "If users clearly feel they need a solution for rapid document sharing/online services/hardware, can this be included into the company's IT policy?"
- "Is there a shadow IT option currently in use in the organization that satisfies compliance needs?"
- "Can you integrate shadow IT (certain apps or services or devices) into your IT assets and install the proper security measures around them?"

The IT department should consult and work with the office of security (if applicable) on any shadow IT implementations to make sure that best security practices are put into place.

When it comes to securing information, the IT department will be responsible for following Tech Pro Research's Information Security Policy and Cloud Data Storage Policy and ensuring users do so as well.

Where possible, the IT department should use SSO for shadow IT deployments, so as to reduce the number of accounts utilized by employees and to help centrally manage access.

Where possible, the IT department should arrange the backup of any information stored in a shadow IT solution (or ensure that existing processes provided by the vendor/host work as expected).

The IT department should utilize network monitoring/firewalls/policies (Active Directory Group Policy, for instance) to verify that unauthorized applications or services are not being used. It is recommended to make a list of approved programs/services, then block third-party applications that might be used to violate this policy.

The IT department is responsible for maintaining and updating this policy (or will designate authorized personnel to do so).

## Monitoring

The IT department will monitor for adherence to this policy. Any change to the policy must be approved by IT, the office of security, or other groups designated as being responsible for revisions or updates.

## Violations and penalties

Violations of the Shadow IT Policy must be immediately reported to any involved managers and the HR department. Violating this policy or any of its tenets could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under local, state, and federal laws.

# Acknowledgment of Shadow IT Policy

This form is used to acknowledge receipt of and compliance with the company's Shadow IT Policy.

## Procedure

Complete the following steps:

1. Read the Shadow IT Policy.
2. Sign and date in the spaces provided.
3. Return a copy of this signed document to the Human Resources department.

## Signature

Your signature attests that you agree to the following terms:

I. I have received and read a copy of the Shadow IT Policy and I understand and agree to the same.

II. I understand the organization may monitor the implementation of and adherence to this policy to review the results.

III. I understand that violations of the Shadow IT Policy could result in termination of my employment and legal action against me.

*Employee Signature* *Employee Title*

*Employee Name* *Date*

*Department/Location*

*Disclaimer: This policy is not a substitute for legal advice. If you have legal questions related to this policy, see your lawyer.*

# About Tech Pro Research

Tech Pro Research provides the information that IT leaders need to make informed decisions and solve today's toughest IT problems. We encourage you to explore all we have to offer:

- Original, in-depth research reports on global IT trends
- Analyst briefings on the latest tech from industry experts
- Ready-made, time-saving policies, templates, and tools
- Comprehensive ebooks compiled from the best of TechRepublic and ZDNet (our award-winning sister sites)

Visit us at www.techproresearch.com.