Enfortris
Technology Services

The Core IT Policies

In a world of complex and ever evolving systems, there is certainly no shortage of things that can go wrong, nor a myriad of thousand-page books on how to address most of them. But in my experience, most organizations would benefit greatly if they just established and followed a few core policies. In this article, I provide an overview of the policies I think are the most important, and why I think so.

1. **Information Use Policy**
   An information use policy essentially outlines what is considered acceptable and, more aptly, unacceptable, for users utilizing an organization's resources. In many cases, it establishes that use of the organization's information resources is for business use only, and explicitly prohibits personal use and malicious activity. It also typically includes some form of activity monitoring consent, and in some cases, the policy will include information classification levels (e.g. public, confidential) and the respective custodial responsibilities of information in the levels. In addition to distribution through normal policy awareness, this policy normally appears in a pared form on IT asset login screens.

   The distribution of an information use policy and the repeated acknowledgements by users upon login serves to remind users to act professionally when using an organization's resources. Additionally, though I am not a lawyer, my understanding is that this policy establishes a legal basis for prosecution for misuse of corporate information systems, such as for porn, fraud, or hacking/breach activity.

2. **IT Access Policy**
   An IT access policy serves as the central standard for how users access IT resources. More elaborately, it defines the different types of users (e.g. business/functional, administrators, customers) and the access levels (e.g. normal, limited, privileged). Additionally, this policy also typically contains authentication standards, such as for password complexity, account lockout, or single sign-on. The better of these policies also mandates periodic review of access to information systems to ensure that only appropriate users can access the organizations information assets.

   This policy centrally defines how an organization's information is accessed, which inherently makes it very important. And periodic review of access is absolutely necessary. It's obvious that a review would identify a former customer or employee that no longer requires access to certain information. But what is less obvious is the business user or administrator that has transferred internally and has accumulated an unduly amount of access to resources. Access standards serve to ensure that users only get the access they need. Periodic reviews serve to ensure that this remains so.

3. **Network Security Policy**
   Firewalls, routers, and wifi, oh my! Cousin to an IT access policy, a network security policy defines what devices can connect to an organization's network, and how. Quite frankly, without appropriate network protections, a modest hacker can attach a device to an organization's network and access its informational resources. This policy typically includes provisions for network device access, network logging and monitoring, intrusion detection/prevention systems (IPS/IDS), and in some cases, standards for various network segments (i.e. DMZ, core, B2B intranet).

   A network security policy serves to make it more difficult for hackers to access an organization's information. Practices such as vulnerability scanning and penetration testing are (appropriately) becoming increasingly demanded to prevent uninvited users from gaining access to resources. The first line of defense in this area is the implementation of a good network security policy.

4. **Systems Maintenance Policy**
   The systems maintenance policy serves as the central management standard for an IT environment. It typically contains standards for the following:
   a. Asset management: This section outlines how assets are tracked, and normally has provisions for procurement and retirement. It's easy to keep track of 10, 20, and perhaps even 30 assets. But when IT

systems exceed that quantity, a formal inventory management process is necessary to keep tally of the organization's IT assets. Larger organizations employ a configuration management database (CMDB) with network discovery, or other automated systems to address this challenge. Regardless of the method, an accurate inventory is paramount. Put simply, if your IT inventory is inaccurate, your systems are not being appropriately managed.

b. Version Support: This section outlines an organization's standards for use of third-party products. Due to a lack of such a policy, many organizations are using IT products that are no longer supported by the supplier. So when things go bump in the night, the organization is often required to perform an emergency upgrade before the supplier will begin to address the actual cause of the bump. This causes additional downtime, and things get even more complicated if the old hardware doesn't support the new software. On the other end of the spectrum, brand new versions may have undiscovered flaws. As a sweet spot, many companies adopt a "current version minus one" or "it's still supported" approach.
c. Patch Management: Similar to version control, vendor patches (aka hotfixes, security updates, etc.) address both functional flaws and security vulnerabilities. Due to limited resources, many organizations adopt an "if it ain't broke…" or "it won't happen to us" philosophy. We typically read about them in the newspapers. And if we haven't, well, they're likely compromised and haven't realized it yet. After all, the best black hats are undetected.
d. Critical Configuration Review: When organizations deploy systems, hopefully the implementers change the default configurations to address the needs of the organization and also for the best security. However, over time requirements change, the security landscape changes, and an upgrade can reset a configuration. Without a periodic review of system configuration, systems often have unnecessary open vectors.

Routine system maintenance is the bane of many IT administrators. It is a drudging but necessary activity. Unfortunately, this aspect of administration typically suffers due to increased IT workloads and decreased IT resources. Metaphorically, too many IT organizations are in a vicious cycle of constant fire-fighting, thereby sacrificing fire prevention, which results in more fires. To make matters worse, administrators get praised for firefighting, but not really for fire prevention. The organizations that have established systems maintenance practices have fewer issues and are more adaptable to changing technologies and requirements.

5. Change Management Policy

Due to new technologies, system upgrades, and changing business requirements, change deployment is a continuous process. A change management policy outlines provisions to ensure that change deployment has a minimal functional and security impact. This policy typically includes the following:

Development: This section is for organizations that develop systems, or procure third parties to develop systems for them.

a. Business Requirements: Documented business/system requirements foster a clear understanding for development. Good development policies include provisions for documentation and approval of system requirements, as well as tracking of changes to them.
b. Development Alignment: Development can be messy. A process that ensures that development activities align to the approved business requirements results in a better product and fewer defects during testing.
c. Development Activity Tracking: In the world of security, the ability to trace malicious activity to an individual is valuable. A process that ensures accountability for the code implemented deters malevolence, and also provides an efficient way to contact the right developer for any defects.
d. Testing: Most organizations are wise enough to test their changes on a series of test systems prior to deployment to the production environment; this just makes good sense. In the world of development, testing should include the developer (dev/module/smoke testing), independent IT testers (QA/QC), and business users (user testing).
e. Release Tracking and Deployment: On complex systems, requirements (and enhancements) are implemented in batches. Mature development organizations employ a release management function to track the status of the requirements.

Implementation: Regardless of internal development, or deployment of supplier provided systems, all good internal change implementation policies contain standards for the following:

a. Change Request: In addition to record of the request, this contains a description of the change being implemented, with sufficient information to communicate applicability to all stakeholders.
b. Approval: Approval from the stakeholders (business requestor, other impacted parties), including relevant IT personnel (i.e. personnel from other affected IT functions).
c. Testing: Documentation of testing performed, and results.
d. Validation: Procedures to ensure that the system and changes are functioning as intended.
e. Regression: A process to revert the change if necessary.

6. Systems Performance and Monitoring Policy

This policy serves to define how systems will be monitored, the parameters (thresholds) for acceptable performance, and the response standards for exceeded thresholds/downtime (i.e. SLAs). In the world of IT, things go wrong often. Standards for identification and response of performance (and security…though this is another topic entirely) incidents results in less downtime and happier customers. Large companies typically employ enterprise monitoring systems to support this process; smaller companies rely on their managed service providers for this. The best organizations have established quality teams that evaluate the incidents for root cause analysis (RCA) to minimize problem recurrence.

7. Business Resiliency Policy

Business resiliency policies often take a back seat, and they shouldn't. I think that this stems from the disbelief that a meteor will actually hit Earth, let alone an organization's data or operations center (as touted by many auditors), or that the tornado will hit and affect their concrete-walled data center. But, crazy enough, I know of a story where a bird with a caught snake shorted power lines and ultimately rendered a business operations center useless for a few days. Another story involves a busted water pipe that showered a power distribution unit. Then there's the '94 quake, '05 Katrina, and '12 Sandy, just to name a few. In the words of Jurassic Park, "nature will find a way". When it does, you'll be prepared or you won't. The sooner an organization adopts a business resiliency policy, the cheaper it is to architect for it. Another topic of note is that, while IT often gets charged with resiliency, true business resiliency requires coordination of all business functions (e.g. operations, HR, and facilities). At minimum a business resiliency policy contains standards for the following;

a. Definition and priority of business critical processes, systems, and data.
b. Standards for data backup (e.g. methods, frequency) and restoration.
c. Standards for alternate operations processing.
d. Standards for alternate data processing (i.e. Disaster Recovery).

Companies may choose to implement these in different organization and form. Ultimately, the best companies have a culture of defining operational standards for all critical functions and processes to ensure compliance to them. This list just represents the bare essentials, and a good start.

Author:
Shawn Laher
CISA, CISSP, ITILv3
Founder, IT Consultant
Enfortris, LLC …A Technology Services Company
www.Enfortris.com

About Enfortris

Enfortris, LLC is a technology services company, based in Columbus, Ohio, that supports business IT operations, including technical support, security, and compliance. Additionally, Enfortris helps businesses optimize their operations through data analytics.