800-657-7107 | fosterinstitute.com

IT Services Best Practices Checklist

Complete this simple checklist to find out if your company is following IT Best Practices. These best practices will prevent or reduce risks to your organization's information and infrastructure. This list is by no means inclusive, so if you'd like a more thorough, personal IT review, contact Mike Foster of the Foster Institute at 1-800-657-7107 today.

PERSONNEL SECURITY	Yes	No
Does your staff wear ID badges with current photos?		
Are there different ID badges for employees, visitors, and contractors?		
Are background checks required for employees and contractors?		
Is physical and electronic access blocked immediately for former staff/contractors?		

PHYSICAL SECURITY	Yes	No
Is physical access to electronic information systems restricted?		
Are there methods for controlling physical access to secure areas of your facility?		
Are visitors always accompanied by staff while in controlled areas?		
Are computer workstations located away from public areas?		
Is physical access to computing areas and equipment controlled?		
Are computers set to automatically lock after being idle?		
Are passwords required to unlock computers?		
Do you have a procedure to protecting data during equipment repairs?		
Are laptops stored securely?		
Do you have an emergency evacuation plan and is it current?		
Does your emergency plan include who will seal off sensitive areas and how?		

ACCOUNT AND PASSWORD MANAGEMENT	Yes	No
Is access to your information systems, applications and data protected by passwords?		
Do you have policies for creating and maintaining secure passwords?		
Do you require and enforce secure passwords?		

CONFIDENTIALITY OF SENSITIVE DATA	Yes	No
Do you distinguish between sensitive and non-sensitive data?		
Is your organization's most valuable or sensitive data encrypted?		
Do you have a policy for data retention?		
Do you have policies for managing credit card information?		

Do you have policies for managing personal information?		
Do you create retrievable backups of critical information?		
Are your information backups stored securely?		
Do you shred sensitive documents?		
Is your shred bin locked at all times?		
Do you have policies to wipe data from old electronic equipment prior to disposal?		
Do your disposal procedures include making electronic media unusable?		

DISASTER RECOVERY	Yes	No
Do you have a current disaster recovery plan in case of an emergency or incident?		
Are all key staff members aware of their role in the disaster recovery plan?		
Does your plan include who should notify authorities?		
Does the plan specify who will speak to the press/public?		
Does the plan include communication with your employees and their families?		
Does the plan include contact information sorted and identified by incident type?		
Is there a plan for retrieving the backups of your organization's critical information?		

SECURITY AWARENESS AND EDUCATION	Yes	No
Do you provide ongoing IT security education and training to your staff?		
Does your IT training include being alert to possible security breaches?		
Does your IT training include avoiding sharing passwords with others?		
Is your staff trained to identify and protect sensitive physical and electronic data?		

COMPLIANCE AND AUDIT	Yes	No
Do you review and revise your security policies and procedures on a regular basis?		
Are your IT policies/procedures regularly reviewed for compliance with best practices?		
Do you review and test your disaster recovery plan on a regular basis?		

Checklist Results

Take a few moments to review your answers. Every "No" is a potential risk for your organization. To find out how to reduce or eliminate those risks, contact Mike Foster today 1-800-657-7107 for a FREE IT Security Consultation.