|  |  |
| --- | --- |
|  | **ADVANTAGE PROFESSIONAL SERVICES INC.**  **EXECUTIVE SEARCH & Business SOLUTIONS**  ***Specializing In The Energy Industry***  **recruitment  ABORIGINAL RELATIONS**  **GOVERNANCE  RISK & COMPLIANCE** |

**Description: Checklist for Basic IT Polices & Guidelines**

Description: You may be overwhelmed by the thought of creating IT policies, particularly if you don't have a firm grasp of technology. Here are six basic areas of IT that you should strongly consider implementing to safeguard your organization. When considering policies and guidelines ensure they work for your company and your employees, and they need to be enforced.

If you are not sure how to do this, your company may want to call Simon Reynolds, IT Governance Partner at Advantage Professional to make recommendations for policies according to how technology is used on a daily basis for your business www.advantageprofessional.ca

There are six basic areas of IT that need to be addressed no matter your size.

* **Acceptable Use of Technology**:
* Guidelines for the use of computers, fax machines, telephones, internet, email, and voicemail and the consequences for misuse.
* Policy governing the use of personal devices at work (BYOD). See our sample policy for guidance.
* **Security**:
* Guidelines for passwords, levels of access to the network, virus protection, confidentiality, and the usage of data. Ensure that you map the individual users job profile to their access within your systems. See our sample policy under "Password Policy under the IT Policy & Guidelines section.
* **Disaster Recovery**:
* Guidelines for data recovery in the event of a disaster, and data backup methods. Ensure all your data is not stored on site but rather in a remote site not located in the same community as you. Ensure you visit and test the remote back up at least quarterly. Cloud storage can be an option.
* **Technology Standards**:
* Guidelines to determine the type of software, hardware, and systems will be purchased and used at the company, including those that are prohibited (for example, instant messenger or mp3 music download software).
* Ensure that someone in your organization doesn't decide to purchase software that is not compatible with your system.
* Ensure that all devices are current in their virus protection prior to connecting with your operating system. Installing these detection alerts can save an organization unwanted viruses.
* **Network Set up and Documentation**:
* Guidelines regarding how the network is configured, how to add new employees to the network, permission levels for employees, and licensing of software.
* Ensure you keep track of the access cards, passwords that you give to any individual (see our Password Policy Sample for more details).
* Ensure that all access cards are terminated when someone leaves-EVEN those that have not been returned. Having the list will prevent anyone from gaining access remotely to your systems after they have been terminated/resigned.
* Ensure user passwords can only be changed by IT so your company will always have a means of logging in to anyone's company devices.
* **IT Services**:
* Guidelines to determine how technology needs and problems will be addressed, who in the organization is responsible for employee technical support, maintenance, installation, and long-term technology planning. This is critical for a successful disaster recovery policy.