BallotOnline's IT Policies and Procedures Manual is available under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license. © 2018, University of Maryland University College

BallotOnline
IT Policies and Procedures Manual

Table of Contents

Introduction

The following policies and procedures are designed to help all employees of BallotOnline with the use and purchase of information technology assets and resources within the company.

The policies and procedures, when followed consistently, provide a standardized system for acquiring and utilizing technology assets (hardware and software) by employees. These policies and procedures benefit BallotOnline by ensuring that our IT infrastructure is enhanced and maintained in an efficient and consistent manner, that costs are controlled and justified, and that our IT resources are integrated. The policies and procedures also assist employees by providing clear guidelines and procedures for all IT-related activities.

This document will be amended and expanded to ensure that the policies and procedures align with current business activities.

These policies and procedures apply to all employees.

Acceptable Use of Technology Policy

P&P No.:IT_01

Policy Date: 01/03/2008

Last Revision Date: 06/20/2016

Applies to the following employees:

All users of computer technology and resources owned by BallotOnline.

Policy Objectives

The purpose of the Acceptable Use of Technology Policy is to define the rules that govern the use of all computer technology and resources at the company. These rules are designed to protect both BallotOnline and its employees from intentional or unintentional misuse of computer equipment. Failure to adhere to this policy exposes BallotOnline and its employees to numerous risks, including computer viruses, hacking of network systems and services, and legal liability.

Procedures

This policy applies to employee use of all computer systems, both Internet and intranet, owned by BallotOnline, including but not limited to desktop systems, laptops and notebooks, software, operating systems, storage media, computer peripherals, and network accounts providing electronic mail, web browsing, and FTP.

1. Acceptable Use:

    a. Employees should use only the computer systems, network accounts, and computer applications and files which they are authorized to use.

    b. Employees may not use another employee's network account or attempt to steal or ascertain another employee's password (see Password Security Policy).

    c. Employees are responsible for all computer resources assigned to them, including both hardware and software, and shall not enable or assist unauthorized users to gain access to the company's network by using a computer—either owned by BallotOnline or the employee—that is connected to the network.

    d. Employees must employ system-level and user-level passwords that comply with the company's Password Security Policy. Employees must not share their passwords with other employees or nonemployees and must take all reasonable steps to protect their passwords and secure their computer systems against unauthorized use.

e. Employees must take extreme caution when opening or downloading e-mail attachments sent by unknown parties, since these may contain malware and viruses that may damage or degrade the company's computer systems and network.

f. Employees must comply with all contractual and licensing agreements with respect to third-party resources, both hardware and software, in use at the company.

g. Employees may not attempt to gain access to protected/restricted portions of the company's network or operating system, including security software and administrative applications, without authorization.

h. Employees must not use the company's computer resources to deploy programs, software, processes, or automated transaction-based commands that are intended to disrupt other computer or network users or damage software or hardware components of a system.

i. Employees must comply with the policies and procedures for all computer resources to which they have been given access.

j. Employees are responsible to promptly report any theft, loss, or unauthorized access of the company's network system, or illegal disclosure of any proprietary information.

k. BallotOnline reserves the right to audit computer systems and networks at any time to ensure that employees fully comply with this policy.

2. Fair Share of Resources:

a. Employees may not deploy any automated programs or processes in an attempt to gain technical advantage over other employees at BallotOnline.

b. Employees may not store personal photos, movies, music, and unauthorized software on their computer systems or the company's networks, thereby limiting storage space and possibly degrading the performance of computer systems for other users.

c. BallotOnline may choose, at any time, to set limits on an employee's use of computer and network resources through such means as quotas and time limits, to ensure that the company's resources are available equally to all employees.

3. Compliance with Federal, State, and Local Laws:

a. Employees using BallotOnline's computer and network resources must comply with all federal, state, and local laws.

b. Employees are prohibited from downloading, storing, displaying, or distributing any content that other employees would consider offensive, intimidating, hostile, or sexually demeaning.

c. Employees are prohibited from using BallotOnline's computer and network systems to conduct activities that violate federal, state, or local laws.

d. Employees must comply with all copyright laws and licenses entered into by BallotOnline with respect to hardware and software agreements for third-party materials.

e. Employees must comply with copyright law as it pertains to videos, music, games, images, text, and other media for both personal use and purposes of conducting business at the company.

f. Employees may not use, copy, modify, or distribute copyrighted works, including content from websites, trademarks, and logos, unless they have a legal right to such activities or have secured explicit permission from the copyright holders to undertake such activities. Failure to adhere to this policy may put the company at legal risk, including civil litigation and criminal prosecution.

4. Privacy:

a. Employees using BallotOnline's computer and network systems must respect the privacy and personal rights of other employees at the company.

b. Employees may not access, copy, or distribute another employee's e-mail, data, programs, or other computer files without the express permission of the Director of IT Systems Support.

c. Information that employees create while working at BallotOnline is the property of the company, not the individual employee, and thus employees must adopt and enforce standards that protect the privacy and confidentiality of such information.

d. Employees who are supervisors or custodians of personnel data, such as the Human Resources Department, must adopt rigorous procedures to maintain the confidentiality of such information, including salary, performance evaluations, disciplinary actions, family records, social security numbers, and medical records. Unauthorized or illegal release or distribution of such data is prohibited.

e. All technology resources and their components or peripheral parts are the property of BallotOnline. Access to such resources is limited to authorized users and is for approved purposes only. Employees understand and agree that there is no expectation of privacy when using any of the company's computer and network resources, including e-mail, telephone, text messaging, social media applications, storage devices, and other media.

For questions, contact:

IT Systems Support

Hardware Purchasing Policy

P&P No.: IT_02

Policy Date: 11/20/2015

Last Modified Date: 03/05/2017

Applies to the following employees: Managers

Policy Objectives

To provide guidelines for the purchase of hardware technology to ensure that such technology is appropriate, is priced according to IT standards, and where necessary integrates effectively with other hardware in use at the company. A key goal of the policy is to ensure that the company's hardware is standardized as much as possible, to avoid a mismatched inventory of computer equipment that requires additional time and resources to support. The policy also provides guidelines for ordering new hardware to streamline the ordering process.

Procedures

These procedures apply to the following types of hardware equipment: PC desktop systems, servers, laptops/notebooks, printers, other computer peripherals, and mobile devices.

General:

1. Hardware equipment items over $500 must be budgeted and approved by senior management.
2. Hardware equipment items over $50,000 will go through a competitive bidding process.
3. Hardware purchase requests can only be submitted by department managers and above.
4. All hardware purchase requests must be submitted using the Hardware/Software Purchase Request Form.
5. Managers should allow at least 5 working days for IT to fulfill requests for new hardware equipment.
6. Installation of new equipment will be completed on a date agreed to by both the IT department and department manager.

Specific Steps:

1. The department manager should conduct a thorough assessment of the hardware equipment needs.
2. Complete the Hardware/Software Purchase Request Form. Provide complete answers to each question and write "NA" next to items in the form that do not apply (do not leave items blank).
3. If completed by another employee, department manager reviews and approves (signs/dates) the request form.
4. Submit the request to IT Systems Support for review.
5. IT Systems Support will review the submitted equipment request and take one of the following steps: a) approve the request as submitted and fulfill the order; b) seek additional information about the request; or c) deny the request.

Specific Hardware Procedures

Servers:

1. Servers can only be requested and purchased by the Vice President, IT Systems Support.
2. All new server systems must be compatible with existing computer hardware in use at the company.
3. All new server systems must be supported by a guarantee and/or warranty that meets the company's warranty standards (see standards document) and be compatible with existing servers in use at the company.
4. Deviations from the above requirements can only be approved by the Vice President, IT Systems Support.

Desktop Systems:

1. Newly purchased desktop systems must run on Windows 10 and above operating system and be compatible with existing server, network, and peripheral systems at the company.
2. New desktop systems must be purchased as a bundle, including the computer processor, monitor, keyboard, mouse, speakers, and camera.
3. New desktop systems will include a basic software package, including Windows 10 operating system, Microsoft Office 365, and the current version of Adobe Reader.

4. Preferred provider of desktop systems will be HP and Dell.
5. All new desktop systems must be supported by a guarantee and/or warranty that meets the company's warranty standards (see standards document here).
6. Any deviations from the above requirements must be approved by the department manager and IT Systems Support.

Portable Computer Systems (laptops, notebooks, etc.):

1. Newly purchased laptop or notebook computers must run on Windows 10 and above operating system and be compatible with existing server, network, and peripheral systems at the company.
2. New laptops or notebooks will include a basic software package, including Windows 10 operating system, Microsoft Office 365, and the current version of Adobe Reader.
3. Preferred provider of desktop systems will be HP and Dell.
4. All new laptops and notebooks must be supported by a guarantee and/or warranty that meets the company's warranty standards (see standards document here).
5. Any deviations from the above requirements must be approved by the department manager and IT Systems Support.

Computer Peripherals (printer, scanner, external HD, etc.):

1. BallotOnline provides access to a number of printer stations throughout the workspace. As such, the purchase of personal printers will only be approved for employees whose work is often confidential.
2. The purchase of personal printers must be approved by the Director, IT Systems Support.
3. Computer peripherals must be compatible with existing server, network, and other systems at the company.
4. All new peripherals must be supported by a guarantee and/or warranty that meets the company's warranty standards (see standards document here).
5. Any deviations from the above requirements must be approved by the department manager and IT Systems Support.

Mobile Phones:

1. With few exceptions, only director-level employees and above will be eligible for company-sponsored mobile phones.

2. All mobile phones will operate on the company's current carrier (Verizon).
3. New mobile phone purchases must be approved by the Vice President, IT Systems Support.
4. New mobile phones can be either Android (Samsung) or Apple OS (iPhone) devices.
5. Employees should use their mobile phones for business purposes and direct all personal, nonbusiness calls, text, e-mail, etc., to their personal mobile devices.
6. Employees must not install apps and other programs on their business phones beyond what is required for business purposes. A list of approved business-related apps is available from IT Systems Support.
7. Mobile device accessories, such as a "hands-free kit," must be submitted with the original purchase request for the mobile phone.
8. Any deviations from the above requirements must be approved by the Director, IT Systems Support.

For questions, contact:

IT Systems Support

Software Purchasing Policy

P&P No.: IT_03

Policy Date: 01/03/2008

Last Revision Date:12/08/2017

Applies to the following employees:

Managers

Policy Objectives

To provide guidelines for the purchase of new software technology to ensure that such technology is appropriate for the purchasing department, is priced according to IT standards, and where necessary integrates effectively with hardware and other software programs in use at the company. A key goal of the policy is to ensure that the company's software is standardized as much as possible, to reduce costs and IT support for such technology. The policy also provides guidelines for ordering new software to streamline the ordering process.

Procedures

This policy applies to all software purchased and used by BallotOnline employees, including software that is purchased, leased, obtained under "shareware" or "freeware" arrangements, acquired from vendors or suppliers, or developed in-house.

1. Software purchases over $10,000 will go through a competitive bidding process.
2. All software purchases or download/installation (for free software) must be submitted using the Software Acquisition Form to IT Systems Support for approval, before software is installed on any employee computer system.
3. Department managers must indicate the number of licenses required on the Software Acquisition Form for each program being acquired.
4. Department managers must approve and sign the Software Acquisition Form prior to submitting to IT Systems Support for approval.
5. New software must be compatible with either the individual employee's or the department's computer system to be approved for purchase or acquisition.
6. Once licenses are acquired, all new software must be installed by an IT Systems Support team member, not the purchasing department employee or manager.

Department managers should contact IT Systems Support to schedule a date for the installation.

7. Following the installation of software, any media, licensing keys, and agreements must be acquired by IT Systems Support for storage and control.
8. Employees must not install or attempt to install copies of any software program on computer systems, either business or personal, beyond what is provided for in the software license. Department managers should contact IT Systems Support if additional user licenses are required for any software program.
9. Any deviations from the above requirements must be approved by the Director, IT Systems Support.

For questions, contact:

IT Systems Support

Bring Your Own Device Policy

P&P No.: IT_04

Policy Date: 10/15/2009

Last Revision Date: 04/10/2015

Applies to the following employees:

All employees

Policy Objectives

The purpose of this policy is to provide guidance and oversight for employees' use of personal laptops, notebooks, tablets, mobile phones, and other portable media in the workplace at BallotOnline. The company recognizes the value in allowing employees to bring their own portable devices to work, in terms of job satisfaction and productivity. However, we also recognize the risk to both the company and employee when workers are allowed to use their own computing devices at work. This policy is meant to minimize those risks while maximizing the benefits in allowing employees to bring their own devices to work. All staff who use the company's technology and equipment must adhere to the conditions of this policy.

Procedures

1. The following types of portable technology are approved for use in the workplace at BallotOnline: laptop computers, notebooks, tablets, smartphones (iPhones and Android devices), and webcams.
2. The following types of portable technology are prohibited from use in the workplace at BallotOnline: removable storage devices, such as external hard drives, memory sticks, flash drives, and other similar devices.
3. Employees must first register their personal device with IT Systems Support before they begin using that device at work.
4. Employees agree that IT Systems Support can install mobile device management technology (MDM) on each device they bring to work, in order to establish a virtual wall between personal data and business date on each device.
5. Only manager-level and above and employees who must travel often for work are allowed to bring and register personal devices in the workplace.

6. Employees agree to adhere to the terms of the company's Acceptable Use of Technology Policy in all respects when using approved personal devices at work.
7. Employees agree that BallotOnline has the right to access, monitor, and delete business data from personal devices used by employees in the workplace.
8. Employees may not access and/or download to their personal devices any sensitive or proprietary company information that they are not authorized to access.
9. Employees must regularly back up all company information stored on their personal devices. Employee-owned devices may not be the only device where company data is stored.
10. Employees agree to make every reasonable effort to protect company information when using their personal devices in public settings. Unauthorized persons may not view or access company information on personal devices in public settings.
11. Employees must implement the company's Password Security Policy on their personal devices used in the workplace and for business purposes.
12. All employee-owned devices used in the workplace must have installed company-approved versions of business software, such as operating systems, office applications (Microsoft Office 365), virus protection, e-mail, FTP, and so on.
13. Employees must notify IT Systems Support immediately if any of their personal devices used at work have been lost or stolen.
14. BallotOnline agrees never to access, monitor, or store employees' personal information from their personal devices used at work unless it has reliable information that an employee has accessed or downloaded unauthorized company information or conducted illegal activities on his/her device at work, or is required to do so by a law enforcement agency as part of a criminal investigation. Employees will be notified first before any of their personal information is accessed by the company.
15. Upon termination of employment, employees must submit all personal devices used at work to IT Systems Management so that all company data can be deleted from each device.
16. Any deviation from the above requirements must be approved by the Director, IT Systems Support.

For questions, contact:

IT Systems Support

Website Policy

P&P No.: IT_05

Policy Date: 07/21/2010

Last Revision Date: 05/09/2015

Applies to the following employees:

Employees who develop and maintain the company website; employees who are authorized to publish, modify, and edit company information on the website.

Policy Objectives

This policy provides guidelines for the regular maintenance of the company's website and for the publishing of any company information on its website.

Procedures

1. The register for the company's website must include and maintain the following records:
    a. List of all domain names registered to the company
    b. Renewal dates for all domain names
    c. List and contact information for all hosting providers
    d. Renewal dates for hosting services
2. The company IT Web Specialist will be responsible for maintaining the website register and ensuring that renewals for domain names and hosting services are met prior to renewal deadlines.
3. All content published to BallotOnline's website must be accurate, truthful, respectful, and timely. It is the responsibility of the Senior Website Editor to ensure that all information published on the company website meets these criteria.
4. It is the responsibility of the IT Web Specialist to install and employ IT-approved website metrics tracking software on the company website and to generate usage reports as requested to maintain the website.
5. It is the responsibility of the Senior Website Editor to ensure that all user and/or customer posted comments adhere to the Terms of Use provisions posted on the website. Any user or customer postings that are offensive will be removed from the website as soon as they are known.

6. All employee blogs published on the company website must be reviewed and approved by the Senior Website Editor before being published.
7. The Senior Website Editor, in consultation with Marketing, will be responsible for ensuring that all content published to the company website adheres to the company's branding guidelines.
8. The following types of information should never be published on the company's website:
    a. Trade secrets and private or confidential information
    b. "Insider" financial information that could be used by others to buy or sell shares of company stock
    c. Personal opinions
9. All user and customer data retrieved from the company's website must adhere to the company's Privacy Policy as described on the website.
10. The following employees are authorized to make changes to the company website:
    a. IT Web Specialist
    b. IT web designers
    c. Senior Website Editor
    d. Website editorial staff

For questions, contact:

IT Web Specialist

Electronic Transactions Policy

P&P No.: IT_06

Policy Date: 01/03/2008

Last Revision Date: 02/25/2017

Applies to the following employees:

Managers and employees in Finance and Legal departments

Policy Objectives

The purpose of this policy is to provide guidelines for executing all electronic transactions conducted on behalf of the company, including procurement of goods and services, electronic funds transfer, electronic contracts, and electronic signatures.

Procedures

Procurement of Goods and Services:

1. All electronic purchases of goods and services by an authorized employee at BallotOnline must adhere to the company's purchasing policy as outlined in the Financial Policy and Procedures Manual.
2. Electronic purchases can only be conducted on Internet sites that are safe and secure. All transactions must use industry-standard encryption technology to ensure that such transactions are private and secure.
3. Payment for all electronic purchases can only be executed using the company credit card or electronic funds transfer by authorized employees at BallotOnline.
4. All electronic purchases requiring e-signatures must adhere to the federal Electronic Signatures in Global and National Commerce Act (and to similar state acts).

Electronic Funds Transfer (EFT):

1. BallotOnline prefers electronic funds transfer rather than company credit card or business check payments whenever possible.
2. EFT payments and receipts must adhere to the company's Financial Policies and Procedures Manual.

3. All EFT payments and receipts must be submitted to BallotOnline's Accounts Payable and Accounts Receivable departments for execution and proper accounting.

4. All EFT payments must be properly authorized and include correct invoice or P. O. numbers.

5. EFT payments can only be executed once payment has been authorized by the department manager.

6. EFT payments cannot be authorized by the same person making the payment.

7. EFT receipts must be reconciled against customer accounts on a weekly basis. Receipts that cannot be reconciled to a customer account within 30 days of receipt must be refunded to the paying party.

Electronic Contracts:

1. All electronic contracts must adhere to the federal Electronic Signatures in Global and National Commerce Act and, where appropriate, to the Uniform Electronic Transactions Act (enacted by 47 states, the District of Columbia, Puerto Rico, and the US Virgin Islands).

2. All contracting parties (vendors, suppliers, customers, contractual employees, etc.) must voluntarily approve to execute a contract electronically and be given the option to "opt-out" and elect to execute a paper contract.

3. All electronic contracts must be reviewed and approved by the company's legal department or legal liaison before they are issued to the contracting party.

4. All alterations to underlying electronic contracts must be reviewed and approved by the company's legal department or legal liaison before being adopted as part of the underlying or original contract.

5. All electronic signatures of contracts must be executed using industry-standard and legally recognized e-signature software.

Electronic Signatures:

1. All electronic signatures of agreements, purchase orders, financial documents, and other electronic transactions at BallotOnline must be executed using industry-standard and legally recognized e-signature software.

2. Parties must be given an option to "opt-out" from using electronic transactions and electronic signatures and elect to use a paper transaction instead.

3. Each electronic signature must be attributable (or traceable) to a person who has the intent and authority to sign the record with the use of adequate security and

authentication measures that are contained in the method of capturing the electronic transaction.

4. Recipients of electronic transactions with BallotOnline must be able to permanently retain an electronic record of the transaction at the time of receipt.

For questions, contact:

Legal Department

IT Service Agreements Policy

P&P No.:IT_07

Policy Date: 01/03/2008

Last Revision Date: 10/24/2016

Applies to the following employees:

IT Systems Support managers and staff

Policy Objectives

The purpose of this policy is to provide guidelines to determine how technology needs and problems at BallotOnline will be addressed and who in the organization is responsible for employee technical support, maintenance, installation, and long-term technology planning.

Procedures

1. IT Service agreements over $30,000 will go through a competitive bidding process.
2. The primary mission of IT Systems Support (ITSS) is to provide the following services to employees at BallotOnline:
    a. Provision of general IT services
    b. Provision of network hardware and software
    c. Provision of software for individual user systems (PCs, laptops, notebooks, etc.)
    d. Maintenance of user accounts, IDs, and passwords
    e. Repairs and maintenance of IT equipment
    f. Provision of mobile phones and plans for mobile phone carriers
    g. Provision of television and multimedia equipment
    h. Intranet design and maintenance
    i. Website design and maintenance
    j. Training of employees in use of IT equipment and software
    k. Long-term technology planning

3. Requests for ITSS services must be submitted via the department's intranet site using the ITSS Request for Service Form. Forms must be completely filled out and approved/submitted by the requesting department manager.

4. ITSS will acknowledge service requests within 1 hour. All service requests are then assigned a priority number (1–4) based on the impact and the urgency of the request. The following list provides a guideline for how quickly service requests will be resolved.

    a. Priority 1: high impact, immediate urgency (resolve in 2 hours)

    b. Priority 2: major impact, high urgency (resolve in 4 hours)

    c. Priority 3: minor impact, medium urgency (resolve in 8 hours)

    d. Priority 4: small impact, low urgency (resolve in 16 hours)

5. ITSS maintains an inventory of equipment (PCs, servers, laptops, printers) that are routinely used in the company. Requests for computer equipment not maintained and supported by ITSS must be approved by the requesting manager and by the Vice President, ITSS. All such purchases must also be line-item budgeted in the requesting department's budget.

6. ITSS maintains network and multiuser licenses to software routinely used throughout the company. Requests for purchases of software note maintained and supported by ITSS must be approved by the requesting manager and by the Vice President, ITSS. All such purchases must also be line-item budgeted in the requesting department's budget.

7. ITSS maintains a monthly schedule of all IT user training sessions on its intranet site. Department managers should register new or existing staff for attendance at one or more of the training sessions. Requests for training in use of equipment or software not covered in the monthly sessions should be handled via the ITSS Request for Service Form.

For questions, contact:

IT System Support

Information Security Procedures Policy

P&P No.: IT_08

Policy Date: 01/03/2008

Last Revision Date: 11/15/2016

Applies to the following employees:

All employees

Policy Objectives

The purpose of this policy is to provide guidelines to protect and maintain the security and confidentiality of the company's information, IT systems, networks, and applications from unauthorized access or misuse by those inside and outside of the organization. The policy also provides procedures to prevent and respond to violence in the workplace.

Procedures

Physical Security Procedures/Clean Desk Policy:

1. Employees will ensure that sensitive and confidential information in both hard copy and digital form is secure and locked away when they are away from their desks or going home for the day.
2. Desktop systems, laptops, notebooks, and other personal computer devices must be locked when employees are away from their desks or going home for the day.
3. Computer workstations must be shut down completely at the end of the workday.
4. File cabinets and desk drawers that contain confidential company information must be locked when employees are away from their desks or at the end of the workday.
5. Laptops, notebook PCs, and other personal computer devices must be locked in cabinet drawers at the end of the workday.
6. Keys to cabinets and drawers must not be left on desks or in unlocked drawers when employees are away from their desks or at the end of the workday.
7. User IDs and passwords should never be written out and left unattended at workstations.
8. When using shared printers or fax machines, sensitive or confidential documents should be retrieved immediately and never left unclaimed at printer or fax machine stations.

9. All sensitive and confidential documents that are no longer in use should either be locked away or shredded at the shredding station.

10. Whiteboards in offices, workstations, or meeting rooms should be erased at the end of each meeting if they include sensitive or confidential information.

11. Mass storage devices, such as CD-ROMs and USB drives, should be secured in a locked drawer when not in use.

Physical Security Procedures/Workplace Violence Prevention:

1. Access to BallotOnline's facilities is controlled by security key cards assigned to each employee on their first day of employment. Access key cards should never be left unattended at workstations or elsewhere and should never be given to other employees or nonemployees for use in our facilities.

2. All visitors to our facilities should be directed to the visitor/registration desk for admission to the building. Employees should not help visitors gain entrance to the building unless or until that person or persons have been cleared by building security at the visitor/registration desk.

3. BallotOnline is committed to preventing workplace violence and to maintaining a safe work environment for all employees and visitors to our facilities. To support this key goal, the company has adopted the following guidelines to deal with harassment, intimidation, or possible violence in the workplace at all times:

    a. All employees, vendors, business associates, and customers must be treated with courtesy and respect at all times.

    b. Employees must refrain from fighting or other forms of physical horseplay that could be dangerous to themselves or others in the workplace.

    c. The company does not tolerate any conduct that threatens, intimidates, or harasses other employees, vendors, business associates, or customers in the workplace. Such conduct by any employee may lead to immediate dismissal from the company and possible criminal response by law enforcement agencies.

    d. BallotOnline resources may not be used to intimidate, stalk, or harass anyone inside or outside of the workplace.

    e. Employees who are the target of or who witness workplace threats, intimidation, or actual violence should report the incident to one or more of the following people: immediate supervisor, security personnel, Human Resources, or any member of the senior management team.

    f. Employees should never place themselves in peril or try to intervene in a violent encounter in the workplace.

g. Any employee who has obtained a restraining order that includes the company's facilities as a protected area should notify Human Resources as soon as the order is obtained.

h. Employees are strongly encouraged to report incidents of intimate partner violence to Human Resources. BallotOnline will make every effort to support victims of partner violence by providing referrals to the company's EAP (Employee Assistance Program) or to other community-based resources.

i. BallotOnline will promptly respond to and investigate all reported threats of violence or incidents of violence in the workplace. The company will never retaliate against an employee who makes a good-faith report of threats of violence or incidents of actual violence in the workplace.

j. Any employee found to be responsible for conducting threats, intimidation, harassment, or actual violence inside or outside the workplace will be subject to immediate disciplinary action, including possible termination from employment.

Physical Security Procedures/Cell Phone Use While Driving:

1. Employees who are issued company cell phones must adhere to the following procedures when driving. These procedures were adapted from the U.S. Occupational and Safety Administration:

    a. Employees should turn off their cell phones or set them to "silent" or "vibrate" before entering a vehicle.

    b. If they must take or make a call, employees should pull the vehicle to the side of the road or to some other safe location and put the car in park before making/taking a call.

    c. Employees should set a temporary voicemail greeting on their cell phone while driving, which notifies the caller that the employee is not available to answer calls or make calls while driving.

    d. Employees should inform customers, business associates, vendors, and others of the company policy regarding cell phone use while driving, so that callers understand why calls may not be returned immediately.

    e. At no time should employees send a text message while driving.

    f. Failure to adhere to the company's policy for use of cell phones while driving will result in disciplinary action, up to and including termination from employment.

Physical Security Procedures/Concealed Weapon:

1. Employees may not possess or use any weapon on company properties or in locations where the company conducts business, such as customer/client locations, trade shows, restaurants, company events, and so on.

2. For purposes of this policy, weapons include, but are not limited to: guns, knives or swords with blades more than four inches in length, explosives, and any chemical whose purpose is to cause harm to another individual.

3. These restrictions hold true regardless of whether the employee holds a concealed weapons permit or is allowed by law to possess a weapon.

4. In some cases, possession of a weapon can be authorized by the president of the company for security personnel or a trained employee for purpose of securing the employees and property of BallotOnline. Only the president, or his/her appointee, may make this authorization.

5. BallotOnline will not restrict an employee from transporting or lawfully storing a concealed weapon in his or her privately owned vehicle, while the vehicle is in company-designated parking areas, if the following conditions are met:

    a. The weapon is kept inside the vehicle and out of sight, locked in a compartment, container, or inside the vehicle; and

    b. The employee has a concealed weapons permit

6. Employees who violate this policy will be subject to disciplinary action, up to and including termination from employment.

Information Security Procedures:

1. All employees at BallotOnline are personally responsible for protecting sensitive and confidential information that they use from unauthorized access and/or use.

2. All employees at BallotOnline are responsible for protecting their passwords and other access credentials from unauthorized use.

3. Use and access to BallotOnline information must be for company-authorized use.

4. Access to systems that handle confidential BallotOnline information must be by authorized users and for authorized company use.

5. All employees authorized to access and use BallotOnline confidential information must be trained in the proper procedures for protecting such information.

6. All users of BallotOnline confidential information and resources must be individually identified.

7. Sensitive and confidential information owned by BallotOnline must be protected and secured on all computer systems and devices.

8. All servers that store sensitive and confidential information owned by BallotOnline must be protected against unauthorized access.

9. All servers that store sensitive and confidential information owned by BallotOnline must be physically secured against vandalism and damage to property caused by individuals or acts of nature.

10. Both digital and physical records that include sensitive and confidential BallotOnline information must be protected and secured during transport or transmission.

11. It is the responsibility of IT Systems Support to ensure that all software and other applications that store company sensitive and confidential information is up to date.

12. Protocols must be established that limit the number of unsuccessful attempts to log on and access either an application or a server that stores company sensitive and confidential information.

13. All digital or physical records that include company sensitive and confidential information must be properly destroyed so that such information cannot be retrieved.

14. The company must routinely conduct due diligence to ensure that third parties that store or have access to BallotOnline information or resources have information security procedures in place that meet or exceed those procedures in place at BallotOnline.

15. Employees must report any unauthorized access to or theft of BallotOnline information or resources immediately, once such incidents are known.

Technology Security Procedures:

1. Remote Access:

    a. All BallotOnline employees, contractors, vendors, suppliers, and business associates with remote access to the company's servers and networks will ensure that their remote access security protocols are given the same consideration as their on-site protocols.

    b. When accessing BallotOnline's servers and networks from a personal computer, authorized users are responsible for preventing access to company information and resources by nonauthorized users.

    c. Remote access to BallotOnline's servers and networks by authorized users for illegal activities is prohibited.

    d. Remote access to BallotOnline's servers and networks by authorized users for outside business interests is prohibited.

    e. Remote access to BallotOnline's servers and networks must be controlled with encryption and strong pass-phrases.

    f. All authorized remote access users must have the most current and state-of-the-industry antivirus software installed on their computer systems.

g. Personal equipment used to remotely access BallotOnline's servers and networks must meet the requirements of the company-owned equipment.

2. Wireless Communication:
   a. All wireless communication devices used at a company site and connect to a company network that stores sensitive and confidential information must:
      i. Meet industry standards for performance and security
      ii. Be installed, supported, and maintained by IT Systems Support
      iii. Use company-approved authentication protocols
      iv. Use company-approved encryption protocols
      v. Maintain a hardware address that can be registered and tracked
      vi. Not interfere with other wireless access deployments in the company
3. Server Security:
   a. All servers must be registered within the company-wide enterprise management system. To positively identify points of contact, the following is required at a minimum:
      i. Server contacts and location, as well as a backup contact
      ii. Hardware and OS version
      iii. Main functions and applications
   b. Information in the corporate enterprise management system must be kept up to date.
   c. All configuration changes to production servers must adhere to the appropriate change management procedures.
   d. Authorized employees should routinely monitor and audit equipment, systems, processes, and network traffic for security, compliance, and maintenance purposes.
   e. The following configuration requirements must be adopted for all company servers:
      i. OS configuration must be in accordance with company-approved guidelines
      ii. When applicable, servers and applications not in use must be disabled
      iii. Access-control methods, such as a firewall, must be used to log and protect access to services
      iv. The most current security patches must be installed on all servers
      v. Avoid trust relationships between systems, since they are a security risk

vi. Use only standard security principles of least required access to perform a function

vii. Servers must be physically located in an access-controlled location

viii. It is prohibited from operating servers from an uncontrolled cubicle or workstation environment

4. Software Installation:
    a. Employees may not install software on company computer systems. All software installations must be performed by IT Systems Support staff.
    b. All software requests must be made by department managers according to the Software Purchasing Policy (see above).
    c. Software must be selected from an approved list of applications maintained by IT Systems Support; acquisition of software not included on the approved list must be approved by the Director, IT Systems Support.

For questions, contact:

IT System Support

IT Emergency Management Policy

P&P No.:IT_09

Policy Date: 05/04/2011

Last Revision Date: 04/28/2015

Applies to the following employees:

IT Systems Support employees, members of Emergency Management Response Team, and all managers

Policy Objectives

The purpose of this policy is to ensure that IT Systems Support and its employees are prepared for and can immediately and effectively respond to an emergency situation, either caused by humans or a natural disaster, and that a plan is in place to mitigate any disruptions to the company's technology infrastructure and can resume normal business operations as quickly as possible.

Procedures

General:

1. The IT Emergency and Disaster Recovery Manager will be responsible for directing all IT disaster recovery activities in the event of an emergency.
2. The IT Emergency and Disaster Recovery Manager will represent company-wide IT Systems Support on the Emergency Management Response Team.
3. Each IT division must develop and maintain an Emergency Management Plan, including notification procedures.
4. Each IT division shall account for its employees in the case of a building evacuation. IT supervisors will be responsible for directing the employees under their supervision.
5. The IT Emergency and Disaster Recovery Manager will be responsible for producing a postmortem report that documents outages, system failures, and recovery responses within 60 days of an emergency event.

Critical Records:

1. IT Systems Support (ITSS) must maintain a comprehensive electronic inventory of all servers, network equipment, relevant configurations, and model information, and the applications they support. It is the responsibility of the Network Administrator to ensure that this electronic documentation is produced and kept up to date.
2. All data backups must be labeled and logged and must be ready for use in the event of an emergency. A subset of the data backups will be encrypted and stored offsite in a secured location beyond the geographical location of the systems that produced the backups. The company's Emergency Management Response Team will determine which subset of data backups must be stored offsite.
3. IT disaster response plans must be stored in a single, comprehensive database.
4. The IT Emergency and Disaster Recovery Manager and other stakeholders must be able to access a copy of the IT emergency and disaster response plans independent of ITSS services or network access.
5. All new or updated IT disaster response plans must be reviewed and approved the IT Emergency and Disaster Recovery Manager.

IT Hardware Failure:

1. Failure of any IT system hardware resulting from an emergency event must be immediately reported to the IT Emergency and Disaster Recovery Manager.
2. The IT Emergency and Disaster Recovery Manager is responsible for directing all necessary actions to respond to and recover from an IT hardware failure as a result of an emergency event.
3. In the event of IT hardware failure, it is the responsibility of the Network Administrator (or the IT employee who discovered the failure) to contact the IT Emergency and Disaster Recovery Manager and provide the following information:
    a. Name/title of person who discovered the incident
    b. Description of incident
    c. Assessment of perceived impact of the incident
    d. The ID numbers of the devices involved in the incident
    e. Contact details of the person who discovered the incident
4. The IT Emergency and Disaster Recovery Manager will determine the severity of the incident (whether it is low impact, such as a localized PC issue, or high impact). If the incident is assessed to be high impact, the IT Emergency and Disaster Recovery

Manager will notify the Emergency Management and Response Team and begin immediately implementing the IT Emergency and Disaster Recovery Plan.

5. The IT Emergency and Disaster Recovery Manager will ensure that relevant communications will take place with all affected users, both before and after implementing the IT Emergency and Disaster Recovery Plan.

6. Once the emergency incident has been resolved, all systems will be tested to ensure that they are functioning normally. Basic connectivity testing will be performed by ITSS, but system functionality testing will need to be conducted by the end users. ITSS will coordinate this process.

7. It is the responsibility of the IT Emergency and Disaster Recovery Manager to conduct tests on planned emergency response procedures every three months to ensure that the emergency procedures are effective and will minimize disruptions to the company's ongoing business.

Virus or Other Security Breach:

1. In the event of a virus, malware, or security breach that affects the company's IT systems, the employee who discovers the incident should report it immediately to the IT Emergency and Disaster Recovery Manager.

2. In the event of a virus attack or security breach, it is the responsibility of the Network Administrator (or the IT employee who discovered the failure) to contact the IT Emergency and Disaster Recovery Manager and provide the following information:

    a. Name/title of person who discovered the incident

    b. Description of incident

    c. Assessment of perceived impact of the incident

    d. The ID numbers of the devices involved in the incident

    e. Contact details of the person who discovered the incident

3. The IT Emergency and Disaster Recovery Manager will determine the severity of the incident (whether it is low impact, such as a localized PC issue, or high impact). If the incident is assessed to be high impact, the IT Emergency and Disaster Recovery Manager will notify the Emergency Management and Response Team and begin immediately implementing the IT Emergency and Disaster Recovery Plan.

4. Types of incidents that might require implementation of the IT Emergency and Disaster Recovery Plan:

    a. Breach of personal information

    b. Denial of Service/Distributed Denial of Service

c. Excessive port scans

d. Firewall breach

e. Virus outbreak

5. The IT Emergency and Disaster Recovery Manager will ensure that relevant communications will take place with all affected users, both before and after implementing the IT Emergency and Disaster Recovery Plan.

6. It is the responsibility of ITSS staff, under guidance of the IT Emergency and Disaster Recovery Manager, to assess the impact of the virus attack or security breach and to immediately take steps to protect all IT systems and resume normal business operations as soon as possible. Based on the severity of the incident, the IT Emergency and Disaster Recovery Manager will determine whether to shut down any or all systems in order to stop an attack in real time and/or the preservation of any potential forensic evidence.

7. Once the incident has been resolved, all systems will be tested to ensure that they are functioning normally. Basic connectivity testing will be performed by ITSS, but system functionality testing will need to be conducted by the end users. ITSS will coordinate this process.

8. The IT Emergency and Disaster Recovery Manager will recommend changes to prevent the occurrence from happening again or spreading to other systems.

9. The IT Emergency and Disaster Recovery Manager will produce a postmortem report of the incident and the company's response/recovery procedures within 60 days of the event. The main purpose of the report will be to update policies and procedures and to take preventive steps to ensure that the incident will not happen again.

Disruption of Website:

1. It is the responsibility of the Director, ITSS, to develop and implement a Website Incident Response Plan and to test the plan every 3 months and keep it up to date.

2. In the event that the company's website has been compromised, by means of distributed DoS attacks, the following steps must be taken immediately:

   a. Notify the website host (ISP) of the disruption in service.

   b. Notify the IT Emergency and Disaster Recovery Manager.

   c. The IT Emergency and Disaster Recovery Manager and ITSS staff will assess the severity of the website attack. If judged to be severe, ITSS will implement the Website Disaster Recovery Plan immediately.

   d. If necessary, take the company website offline to allow time for ITSS to remedy the incident.

e. ITSS should scan all networked computers at BallotOnline to ensure they are not infected with any viruses, malware, spyware, or other hacking programs.

f. ITSS will take all necessary steps to diagnose how the company website was hacked and to restore the site to full functionality in a timely manner.

g. ITSS should implement one or more of the following procedures before restoring the website:

   i. Changing all passwords for access to web applications and databases

   ii. Test backup of website and associated databases and make sure these have not been corrupted

   iii. Use all necessary tools to find and remove malware from the website

   iv. Take other steps to identify and fix the weaknesses that resulted in the website attack

   v. The Emergency and Disaster Recovery Manager will produce a postmortem report of the incident and the company's response/recovery procedures within 60 days of the event. The main purpose of the report will be to update policies and procedures and to take preventive steps to ensure that the incident will not happen again.

For questions, contact:

IT System Support

References

BallotOnline acknowledges the following publications used in crafting its IT policy and procedures manual:

Asia Pacific International College. (2016, December 16). Emergency management of information technology procedures. Retrieved from http://www.apicollege.edu.au/policies/Emergency_Management_of_Information_Techology_Procedures.pdf

Asia Pacific International College. (2016, December 16). IT services agreement procedures. Retrieved from http://www.apicollege.edu.au/policies/IT_Services_Agreement_Procedures.pdf

Asia Pacific International College. (2016, December 27). Website policy. Retrieved from http://www.apicollege.edu.au/policies/Website_Policy.pdf

Brown University, Computing & Information Services. (n.d.). Acceptable use policy. Retrieved from https://it.brown.edu/computing-policies/acceptable-use-policy

Chellakari, K. (2012). Developing a BYOD policy: Weigh the risks, challenges and benefits. Retrieved from http://searchsecurity.techtarget.com/feature/Developing-a-BYOD-Strategy-Weigh-the-Risks-Challenges-and-Benefits

CSO. (2016). Security policy samples, templates, and tools. Retrieved from https://www.csoonline.com/article/3019126/security/security-policy-samples-templates-and-tools.html

CSO. (2016, January 11). Sample cell phone use while driving policy. Retrieved from https://www.csoonline.com/article/3020581/security/sample-cell-phone-use-while-driving-policy.html

Grant Thornton. (n.d.). *Information Technology Policy and Procedure Manual Template*. Melbourne, Australia: Business Victoria. Retrieved from https://www.business.vic.gov.au/__.../IT-policies-and-procedures-manual- template.docx

Heathfield, S. M. (2016, October 27). Concealed weapons sample policy. Retrieved from https://www.thebalance.com/concealed-weapons-sample-policy-1918872

International Legal Technology Association. (n.d.). IT incident response plan. Retrieved from https://www.iltanet.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=966e76a0-5664-43b6-9f3e-fa0540055508&ssopc=1

Lannon, P. G., & Schreiber, P. M. (2016, February 1). BYOD policies: What employers need to know. Retrieved from https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx

Maurer, R. (2015, May 19). Distracted driving policies save lives, protect organizations. Retrieved from https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/distracted-driving-policies-save-lives.aspx

Maynard, Cooper & Gale LLC. (n.d.). Sample firearm policy. Retrieved from https://alabamaretail.org/wp-content/uploads/sample-weapons-policy.pdf

Northeastern University. (n.d.). Policy on use of electronic signatures. Retrieved from https://www.northeastern.edu/policies/pdfs/Policy_on_Use_of_Electronic_Signatures.pdf

Privacy Rights Clearinghouse. (2014). Bring your own device (BYOD) . . . at your own risk. Retrieved from https://www.privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk

SANS Institute. (2014). Acceptable use policy. Retrieved from https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy

SANS Institute. (2014). Clean desk policy. Retrieved from https://www.sans.org/security-resources/policies/general/pdf/clean-desk-policy

SANS Institute. (2014).Disaster recovery plan policy. Retrieved from https://www.sans.org/security-resources/policies/general/pdf/disaster-recovery-plan-policy

SANS Institute. (n.d.). Information security policy templates. Retrieved from https://www.sans.org/security-resources/policies

Sobolewski, M. D., & Ostrowski, C. R. (2015). E-contracting: What corporate counsel need to know. *NYSBA Inside*. Retrieved from http://www.mclaughlinstern.com/docs/publications/E-Contracting-What_Corporate_Counsel_Need_to_Know.pdf

Sisco, M. (2004). *Practical IT policies & procedures: A quick guide in developing your company's internal policies and procedures*. Columbia, TN: MDE Enterprises.

Society for Human Resource Management. (2014, July 10). Workplace violence prevention policy. Retrieved from https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/cms_007623.aspx

The Tavistock and Portman NHS Foundation Trust. (n.d.). Information communication technology backup and failure contingency procedure. Retrieved from https://tavistockandportman.nhs.uk/documents/73/ict-failure-contingency-plan.pdf

University of Florida, Information Technology (n.d.). Prioritizing service requests & incidents. Retrieved from https://it.ufl.edu/media/itufledu/itsm/prioritizing_in_myit.pdf

University of Greenwich. (n.d.). Purchasing and acquiring software. Retrieved from http://www.gre.ac.uk/it-and-library/about/policies-and-procedures/it-policies/conduct-and-usage/policy/purchasing

University of Southern California. (n.d.) Emergency management: Business continuity and IT disaster recovery. Retrieved from https://policy.usc.edu/preparedness/

University of Utah (n.d.). Policy 3-006: Use of eectronic signatures and records, Retrieved from http://regulations.utah.edu/administration/3-006.php

Workforce. (2003). Workplace violence prevention and response policy. Retrieved from http://www.workforce.com/2003/09/18/workplace-violence-prevention-and-response-policy/