Business Continuity Policy

Your Company Name

Notes for Use:

- This Plan is intended for organizations with over ~50-75 people. It can serve as a standalone Policy document, and points to required sub-documents that will collectively comprise the BC “Plan”.
- Identify an Owner for this Policy and ensure that is reviewed and updated at least Annually
- Carefully revise this template to tailor it to your organization.
- This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document
- Please open header and click on picture placeholder (top right) to insert your logo.

Purpose and Scope

1) The purpose of this policy is to ensure that the organization establishes objectives, plans and procedures such that a major disruption to the organization's key business activities is minimized.

2) This policy applies to all infrastructure and data within the organization's information security program.

3) This policy applies to all management, employees, and suppliers that are involved in decisions and processes affecting the organization's business continuity. This policy must be made readily available to all whom it applies to.

Background

1) The success of the organization is reliant upon the preservation of critical business operations and essential functions used to deliver key products and services. The purpose of this policy is to define the criteria for continuing business operations for the organization in the event of a disruption. Specifically, this document defines:

    A) The structure and authority to ensure business resilience of key processes and systems.

    B) The requirements for efforts to manage through a disaster or other disruptive event when the need arises.

    C) The criteria to efficiently and effectively resume normal business operations after a disruption.

2) Within this document, the following definitions apply:

    A) *Business impact analysis/assessment* - an exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to return to a normal level of operation, and prioritizes recovery of processes and the supporting system.

    B) *Disaster recovery plan* - a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a defined time and cost, when an activity is interrupted by an emergency or disaster.

    C) *Recovery time objective* - the amount of time allowed for the recovery of a business function or resource to a normal level after a disaster or disruption occurs.

    D) *Recovery point objective* - determined based on the acceptable data loss in the case of disruption of operations.

Policy

1) *Business Risk Assessment and Business Impact Analysis*

    A) Each manager is required to perform a business risk assessment and business impact analysis for each key business system within their area of responsibility.

    B) The business risk assessment must identify and define the criticality of key business systems and the repositories that contain the relevant and necessary data for the key business system.

C) The business risk assessment must define and document the Disaster Recovery Plan (DRP) for their area of responsibility. Each DRP shall include:

i) Key business processes.

ii) Applicable risk to availability.

iii) Prioritization of recovery.

iv) Recovery Time Objectives (RTOs).

v) Recovery Point Objectives (RPOs).

2) *Disaster Recovery Plan*

A) Each key business system must have a documented DRP to provide guidance when hardware, software, or networks become critically dysfunctional or cease to function (short and long term outages).

B) Each DRP must include an explanation of the magnitude of information or system unavailability in the event of an outage and the process that would be implemented to continue business operations during the outage. Where feasible, the DRP must consider the use of alternative, off-site computer operations (cold, warm, hot sites).

C) Each plan must be reviewed against the organization's strategy, objectives, culture, and ethics, as well as policy, legal, statutory and regulatory requirements.

D) Each DRP must include:

i) An emergency mode operations plan for continuing operations in the event of temporary hardware, software, or network outages.

ii) A recovery plan for returning business functions and services to normal on-site operations.

iii) Procedures for periodic testing, review, and revisions of the DRP for all affected business systems, as a group and/or individually.

3) *Data Backup and Restoration Plans*

A) Each system owner must implement a data backup and restoration plan.

B) Each data backup and restoration plan must identify:

i) The data custodian for the system.

ii) The backup schedule of each system.

iii) Where backup media is to be stored and secured, as well as how access is maintained.

iv) Who may remove backup media and transfer it to storage.

v) Appropriate restoration procedures to restore key business system data from backup media to the system.

vi) The restoration testing plan and frequency of testing to confirm the effectiveness of the plan.

vii) The method for restoring encrypted backup media.

Revision History

Revision date	Action	Approver
1/1/2020	Initial Document	[name], [role]
3/3/2020	Review	[name], [CEO]

Business Continuity Policy

Contact Us www.yourwebsite.com | youremail@example.com

ACCEPTABLE USE POLICY

Your Company Name

Notes for Use:

- This policy is an example only. It will need to be carefully reviewed and revised to fit the risks common to users within your organization.
- After you have created this document:
  - All current employees will be required to acknowledge that they have read it.
  - Any new hires, and if you choose, contractors, should acknowledge this policy upon hire.
  - Retain a non-employee facing version should you ever need to make a revision. If you do make a revision, have all current employees re-sign it.
- This policy does not need to be refreshed and re-signed each year. Request acknowledgement only after a major revision.
- Couple the roll out of this policy with internal communications, such as an email to all hands, a training event, or at an All Hands meeting.
- This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document.
- Please open header and click on picture placeholder (top right) to insert your logo.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at {INSERT FIRM NAME}. These rules are in place to protect the employee and {INSERT FIRM NAME}. Inappropriate use exposes {INSERT FIRM NAME} to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct {INSERT FIRM NAME} business or interact with internal networks and business systems, whether owned or leased by {INSERT FIRM NAME} the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at {INSERT FIRM NAME} are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with {INSERT FIRM NAME} policies and standards, and local laws and regulation. Exceptions to this policy are documented below.

This policy applies to employees, contractors, consultants, temporaries, and other workers at {INSERT FIRM NAME} including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by {INSERT FIRM NAME}.

Policy

General Use and Ownership

- {INSERT FIRM NAME} proprietary information stored on electronic and computing devices whether owned or leased by {INSERT FIRM NAME}, the employee or a third party, remains the sole property of {INSERT FIRM NAME}.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of {INSERT FIRM NAME} proprietary information {TO WHOM}.
- You may access, use or share {INSERT FIRM NAME} proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. {INSERT FIRM NAME} is responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within {INSERT FIRM NAME} may monitor equipment, systems and network traffic at any time.
- {INSERT FIRM NAME} reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- System level and user level passwords must comply with {INSERT FIRM NAME}'s password guidelines: {Insert basic password parameter settings here: e.g. complex, with a capital letter, and ## characters long}. Providing access to another individual, either deliberately or through failure to secure, is prohibited.

- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

- Postings by employees from a {INSERT FIRM NAME} email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of {INSERT FIRM NAME} unless posting is in the course of business duties.

- Employees must use extreme caution when opening email attachments received from unknown senders, to avoid viruses or malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of {INSERT FIRM NAME} authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing {INSERT FIRM NAME} owned resources.

The lists below are by no means exhaustive, but provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by {INSERT FIRM NAME}.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which {INSERT FIRM NAME} or the end user does not have an active license is strictly prohibited.

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5. Using a {INSERT FIRM NAME} computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

6. Making fraudulent offers of products, items, or services originating from any {INSERT FIRM NAME} account.

7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or

account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

9. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

10. Circumventing user authentication or security of any host, network or account.

11. Introducing honeypots, honeynets, or similar technology on the {INSERT FIRM NAME} network.

12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

14. Providing information about, or lists of, {INSERT FIRM NAME} employees to parties outside {INSERT FIRM NAME}.

Email and Communication Activities:

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the Chief Compliance Officer.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within {INSERT FIRM NAME}'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by {INSERT FIRM NAME} or connected via {INSERT FIRM NAME}'s network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

The {INSERT FIRM NAME} team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits. All those found in policy violation may be subject to disciplinary action, up to and including termination.

Employee Acknowledgement (for Employee Facing)

_____ _____

Name/Signature Date

Major Revisions (Non-employee facing)

Revision date	Action	Approver
1/1/2020	Initial Document	[name], [role]
3/3/2020	Review	[name], [CEO]

ACCEPTABLE USE POLICY

Contact Us www.yourwebsite.com | youremail@example.com

Bring Your Own Device Policy

Your Company Name

Notes for Use:

- Carefully revise this template to tailor it to your organization
- It is intended to be signed by all Employees (and Consultants, if appropriate) that use their own devices.
- Update “VP of Engineering” with the role in your Organization.
- Retain a master version of this document in a centralized location and update it as business needs dictate. Include a revision history with the Master version only.
- This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document
- Please open header and click on picture placeholder (top right) to insert your logo.

OVERVIEW

[COMPANY NAME] is required to protect its information assets in order to safeguard its customers, technology infrastructure, intellectual property and reputation. This policy establishes [COMPANY NAME] standards for the use of personally owned electronic devices for work related purposes for employees, independent consultants and contractors (collectively referred to as “users”). Users must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network and company tools (defined collectively as any cloud storage, network drives, email solutions, [COMPANY NAME] owned software solutions, or other IT products for which [COMPANY NAME] owns a license).

SCOPE

[COMPANY NAME] users may have the opportunity to use their personal electronic devices for [COMPANY NAME] work purposes. Personally-owned devices include cell phones, smartphones, tablets, laptops, and computers. In the case of contractors, this device may be one issued by the firm for which they work and not issued by [COMPANY NAME], provided there is a current contract in place. Certain classes of users may have limitations, described below, based on how they interact with the [COMPANY NAME] network, systems, data or tools to conduct [COMPANY NAME] related activities.

POLICY

Expectation of Privacy:

[COMPANY NAME] will respect the privacy of your personal device and will only request access to the device to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads [COMPANY NAME] email, attachments, or documents to their personal device).

This differs from [COMPANY NAME]-provided equipment/services, where users do not have the right, nor should they have an expectation of privacy while using [COMPANY NAME] equipment or services.

No system access to [COMPANY NAME] tools shall be granted until such time as the device has been configured to meet this BYOD policy.

All BYOD Users Shall:

1) Acknowledge the Acceptable Use Policy which governs how [COMPANY NAME] assets are to be used to protect [COMPANY NAME] data.

2) Password protect or otherwise secure their device(s).

3) Maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not “jailbreak” the device by installing software that allows the user to bypass standard built-in security features and controls.

4) Allow [COMPANY NAME] administrators to install JumpCloud security suite (firewall, antivirus, and web site protector applications) on their personal device.

5) Confirm that their device will not be shared with other individuals or family members, due to the business use of the device.

6) Avoid storing or sharing [COMPANY NAME] data onto their personal device and 3rd party services, but rather, rely on cloud storage services provided by [COMPANY NAME] (i.e. Box, Smartsheet, Google Drive, Gmail, Confluence).

   A) In limited cases, data may be temporarily downloaded onto personal devices as long as the [COMPANY NAME] data is later removed/deleted.

7) Notify [COMPANY NAME] Network Team, as soon as practical if unauthorized access to company data has taken place via their mobile device OR if the device has been lost or stolen. IT will lock [COMPANY NAME] related services.

Independent Consultants (ICs) shall:

1) Allow [COMPANY NAME] IT to configure standard apps, such as browsers, office productivity software and security tools, before they can access the network.

2) Not retain personal data of [COMPANY NAME] employees or customers on their device unless contractually allowed to do so.

3) Never backup or transfer [COMPANY NAME] data onto a service not supported by [COMPANY NAME] (such as personal Dropbox or OneDrive Accounts, a memory stick, USB stick or a personal external hard drive).

4) Maintain a password manager at the IC's expense.

5) Maintain a malware and virus protection service at the IC's expense.

Contractors shall:

1) Not retain personal data of [COMPANY NAME] employees or customers on their device, unless contractually allowed to do so.

2) Adhere to all contractual security provisions, per contract between the Contractor and [COMPANY NAME].

[COMPANY NAME] shall:

1) Provide VPN access for all employees (by default) and for other BYOD users with the approval of VP of Engineering.

2) For users' personal devices that are allowed access to corporate email and [COMPANY NAME] Google Drive, [COMPANY NAME] will be granted permission to remotely wipe the device. The SRE Team, in consultation with the VP of Engineering, will determine if a device will need to be wiped based on the risk of confidential information present on the device.

3) Only provide support for [COMPANY NAME] provided devices and licensed software.

4) Reserve the right to inspect any user's personal devices and remove all company tools and data upon termination of employment or contract.

5) Reserves the right to disconnect devices or disable services without notification.

6) Implement BYOD security controls that will ensure the safety and protection of data inline with law and regulations (such as EU GDPR and CCPA).

USER ACKNOWLEDGMENT AND AGREEMENT

It is [COMPANY NAME]'s right to restrict or rescind BYOD computing privileges, or take other administrative or legal action due to failure to comply with the above referenced Policy. Violation of this policy may be grounds for disciplinary action.

I acknowledge, understand and will comply with the above referenced policy as applicable to my BYOD usage of [COMPANY NAME] services.

I understand that the addition of [COMPANY NAME] tools on my device may decrease the available memory or storage on my personal device and that [COMPANY NAME] is not responsible for any loss or theft of, damage to, or failure in the device that may result from the use of third-party software and/or use of the device governed by this policy.

I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility. I understand that [COMPANY NAME] will only provide technical support for [COMPANY NAME] tools.

I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device may not be provided.

Employee Name: _____

BYOD Device(s):

_____

_____

Services to be Used:

_____

_____

_____

_____

_____

Anti-Virus or other Security Software installed on the Device:

_____

_____

_____

Employee Signature: _____ Date: _____

Bring Your Own Device Policy

Contact Us

www.yourwebsite.com | youremail@example.com