Security Policy

Keeping our clients' data secure is an absolute top priority at Botsify Inc.. Our goal is to provide a secure environment, while also being mindful of application performance and the overall user experience across our different applications and solutions.

Botsify platform

End to End Security

Our Botsify platform is hosted on Amazon Web Services (AWS), providing end-to-end security and privacy features built in. Our platform partner team takes additional proactive measures to ensure a secure infrastructure environment. For additional, more specific details regarding AWS security, please refer to https://aws.amazon.com/security/.

Data Centre Security

Amazon Web Services (AWS) maintains an impressive list of reports, certifications, and third party assessments to ensure complete and ongoing state-of-the-art data centre security (https://aws.amazon.com/compliance/programs/). They have many years of experience in designing, constructing, and operating large-scale data centres.

AWS infrastructure is housed in Amazon-controlled data centres throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centres, and the data centres themselves are secured with a variety of physical controls to prevent unauthorized access. More information on AWS data centres and their security controls can be found here: https://aws.amazon.com/compliance/data-center/data-centers/

Application Security

All BotBuild application communications are encrypted over 256 bit SSL, which cannot be viewed by a third party and is the same level of encryption used by banks and financial institutions. All data for BotBuild is encrypted at rest using AES-256 encryption.

Botsify platform partner team actively monitors ongoing security, performance and availability 24/7/365. We run automated security testing on an ongoing basis. We also contract a third party for penetration testing.

Development and Bespoke Development

We use the same principles with bespoke development as we do with the chatbot platform and are partner teams that support the platform.

These are obviously bespoke to each client and are difficult to detail in a general policy, but we can scope and document the details of a specific project on request for the development process and would encourage that within our clients to ensure that they can include it within their own policies with details that are specific to them.

General Security Policy

Botsify Inc. employs strict security standards and measures throughout the entire organization. Every team member is trained and kept up to date on the latest security protocols. We regularly undergo testing, training, and auditing of our practices and policies.

1. Purpose, Scope, and Organization

What is this document, why does it exist, what does it cover, and who is in charge of it?

This policy defines behavioural, process, technical, and governance controls pertaining to security at Botsify Inc. that all personnel are required to implement in order to ensure the confidentiality, integrity, and availability of the Botsify Inc. service and data ("Policy"). All personnel must review and be familiar with the rules and actions set forth below.

This Policy defines security requirements for:

- all Botsify Inc. employees, contractors, consultants, platform partners and any other third parties providing services to Botsify Inc. ("personnel"),
- management of systems, both hardware and software and regardless of locale, used to create, maintain, store, access, process or transmit information on behalf of Botsify Inc., including all systems owned by Botsify Inc., connected to any network controlled by Botsify Inc., or used in service of Botsify Inc.' business, including systems owned third party service providers, and
- circumstances in which Botsify Inc. has a legal, contractual, or fiduciary duty to protect data or resources in its custody.

In the event of a conflict, the more restrictive measures apply.

1.1. Governance and Evolution

This Policy was created in close collaboration with and approved by Botsify Inc. executives. It is reviewed and modified as needed to ensure clarity, sufficiency of scope, concern for client and personnel interests, and general responsiveness to the evolving security landscape and industry best practices.

1.2. Security Team

The Botsify Inc. security team oversees the implementation of this Policy, including

- procurement, provisioning, maintenance, retirement, and reclamation of corporate computing resources,
- all aspects of service development and operation related to security, privacy, access, reliability, and survivability,
- ongoing risk assessment, vulnerability management, incident response, and
- security-related human resources controls and personnel training.

1.3. Risk Management Framework

The security team maintains a Risk Management Framework. Risk assessment exercises inform prioritization for ongoing improvements to Botsify Inc.' security posture, which may include changes to this Policy itself.

Our Risk Management Framework incorporates the following:

- Identification of relevant, potential threats.
- A scheme for assessing the strength of implemented controls.
- A scheme for assessing current risks and evaluating their severity.
- A scheme for responding to risks.

2. Personnel and Office Environment

What are Botsify Inc.' expectations of its personnel and the workplace regarding systems and data?

Botsify Inc. is committed to protecting its clients, personnel, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly in the context of its established employment culture of openness, trust, maturity, and integrity.

This section outlines expected personnel behaviours affecting security and the acceptable use of computer systems at Botsify Inc.. These rules are in place to protect our personnel and Botsify Inc. itself, in that inappropriate use may expose clients and partners to risks including malware, viruses, compromise of networked systems and services, and legal issues.

2.1. Work Behaviours

The first line of defence in data security is the informed behaviour of personnel, who play a significant role in ensuring the security of all data, regardless of format. Such behaviours include those listed in this section as well as any additional requirements specified in the employee handbook, specific security processes, and other applicable codes of conduct.

Training

All employees and contractors must complete the Botsify Inc. security awareness and data handling training programs.

Unrecognized Persons and Visitors

It is the responsibility of all personnel to take positive action to maintain physical security. Challenge any unrecognized person present in a restricted office location. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff and the security team. All visitors to Botsify Inc. offices must be registered as such or accompanied by a Botsify Inc. employee.

Clean Desk

Personnel should maintain workspaces clear of sensitive or confidential material and take care to clear workspaces of such material at the end of each workday.

Unattended Devices

Unattended devices must be locked. All devices will have an automatic screen lock function set to automatically activate upon no more than fifteen minutes of inactivity.

Use of Corporate Assets

Systems are to be used for business purposes in serving the interests of the company, and of our clients and partners in the course of normal business operations. Personnel are responsible for exercising good judgment regarding the reasonableness of personal use of systems. Only Botsify Inc.-managed hardware and software is permitted to be connected to or installed on corporate equipment or networks and used to access Botsify Inc. data. Botsify Inc.-managed hardware and software includes those either owned by Botsify Inc. or owned by Botsify Inc. personnel but enrolled in a Botsify Inc. device management system. Only software that has been approved for corporate use by Botsify Inc. may be installed on corporate equipment. All personnel must read and understand the list of prohibited activities outlined in this Policy. Modifications or configuration changes are not permitted without explicit written consent by the Botsify Inc. security team.

Removable Storage, No Backups, Use of Cloud Storage

Use of removable media such as USB drives is prohibited. Personnel may not configure work devices to make backups or copies of data outside corporate policies. Instead, personnel are expected to operate primarily “in the cloud” and treat local storage on computing devices as ephemeral. Botsify Inc. data must be saved to company-approved secure cloud storage (e.g. SharePoint) to ensure that even in the event of a corporate device being lost, stolen, or damaged, such artifacts will be immediately recoverable on a replacement device.

Prohibited Activities

The following activities are prohibited. Under certain conditions and with the explicit written consent of the security team, personnel may be exempted from certain of these restrictions during the course of their legitimate job responsibilities (e.g. planned penetration testing, systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

- Under no circumstances are personnel of Botsify Inc. authorized to engage in any activity that is illegal under local or international law while utilizing Botsify Inc.-owned resources.
- 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 Botsify Inc..
- Violating or attempting to violate the terms of use or license agreement of any software product used by Botsify Inc. is strictly prohibited.
- 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 Botsify Inc. or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology may result in a violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.
- Revealing your account password to others or allowing use of your account by others. This includes colleagues, as well as family and other household members when work is being done at home.
- Making fraudulent offers of products, items, or services originating from any Botsify Inc. account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties and then only to the extent the warranties are consistent with Botsify Inc.' authorized warranties.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- 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. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious or unlawful purposes.

- Except by or under the direct supervision of the security team, port scanning or security scanning, or other such software designed to exploit or find computer, software, or network vulnerabilities.

- 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.

- Circumventing user authentication or security of any host, network or account or attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.

- Attempting to interfere with or deny service to any other user.

- Providing information about, or lists of, Botsify Inc. personnel to parties outside Botsify Inc..

- Installation of software which installs or includes any form of malware, spyware, or adware as defined by the security team.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.

- Attempts to subvert technologies used to effect system configuration of company-managed devices (e.g. MDM) or personal devices voluntarily used for company purposes (e.g. mobile Work Profiles).

2.2. Personnel Systems Configuration, Ownership, and Privacy

Centralized System Configuration

Personnel devices and their software configuration are restricted by members of the security team via access control. This means that only authorised access can action auditing/installing/removing software applications or system services, managing network configuration, enforcing password policy, encrypting disks, remote wipe & recovery, copying data files to/from employee devices, and any other allowed interaction to ensure that employee devices comply with this Policy.

Data and Device Encryption

All devices must use modern full disk encryption to protect data in the event of a lost device.

Endpoint/Antivirus/Antimalware Protection

Devices must automatically install and configure the Botsify Inc. provided antivirus software for endpoint protection. Configured software will report status and potential threats, allowing for remote administration and reporting by the security team.

Retention of Ownership

All software programs, data, and documentation generated or provided by personnel while providing services to Botsify Inc. or for the benefit of Botsify Inc. are the property of Botsify Inc. unless otherwise covered by a contractual agreement.

Personnel Privacy

While Botsify Inc.' network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Botsify Inc.. Due to the need to protect Botsify Inc.' network, management does not intend to guarantee the privacy of personnel's personal information stored on any network device belonging to Botsify Inc.. Personnel are responsible for exercising good judgment regarding the reasonableness of personal use such as general web browsing or personal email. If there is any uncertainty, personnel should consult the security team or their manager.

Personnel should structure all electronic communication with recognition of the fact that the content could be monitored and that any electronic communication could be forwarded, intercepted, printed, or stored by others.

Botsify Inc. reserves the right, at its discretion, to review personnel's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as corporate policies.

Botsify Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. For security and network maintenance purposes, authorized individuals within Botsify Inc. may monitor equipment, systems and network traffic at any time.

2.3. Human Resources Practices

Background Checks

Background checks are conducted for personnel with access to production infrastructure prior to their start date. The consequences of problematic background check results may range from a limitation of security privileges, to revocation of employment offer, to termination.

Training

The security team maintains a company-wide security awareness program delivered to all personnel. The program covers security awareness, policies, processes, and training to ensure that personnel are sufficiently informed to meet their obligations. Those most responsible for maintaining security at Botsify Inc., including the security team itself as well as key engineering/operations staff, undergo more technical continuing education.

Separation

In the case of personnel termination or resignation, the security team coordinates with human resources to implement a standardized separation process to ensure that all accounts, credentials, and access of outgoing employees are reliably disabled.

2.4. Physical Office Environment

Access to Botsify Inc. offices is mediated by a staffed front office and programmable door control access. All doors shall remain locked or staffed under normal business conditions. The security team may provide approval to unlock doors for short periods of time in order to accommodate extenuating physical access needs.
Internet-based security cameras are positioned to record time-stamped video of ingress/egress, which are stored off-site.

2.5. Office Network

Internet access shall be provided to devices via wired ethernet and WPA2 wifi. Networking switches and routers shall be placed in a locked networking closet with only the security team having access. Botsify Inc. executives and the security team may grant access to the networking closet to individuals on a case-by-case and as-needed basis. A network firewall that blocks all WAN-sourced traffic shall be put in place.
WAN-accessible network services shall not be hosted within the office environment.

3. Personnel Identity and Access Management

How does Botsify Inc. define, control, and maintain user identity and permissions for personnel?

3.1. User Accounts and Authentication

Each individual having access to any Botsify Inc.-controlled system does so via a Microsoft user account denoting their system identity. Such user accounts are required to have a unique username, a unique strong password of at least 8 characters, and a two-factor authentication (2FA) mechanism.

Logging into Botsify Inc. Systems

Logins by personnel may originate only from Botsify Inc.-managed devices. Authentication is performed by Microsoft account management system. Botsify Inc. leverages Microsoft's facilities of detecting malicious authentication attempts. Repeated failed attempts to authenticate may result in the offending user account being locked or revoked.

Logging into Third Party Systems

Whenever available, third-party systems must be configured to delegate authentication to Botsify Inc.' Microsoft account authentication system (described above) thereby consolidating authentication controls into a single user account system that is centrally managed by the security team.

When authentication to Microsoft is not available, unique strong passwords must be created and stored in the Botsify Inc. approved password management system. Passwords must be paired with two-factor/MFA authentication.

Revocation and Auditing of User Accounts

User accounts are revoked (that is, disabled but not deleted) immediately upon personnel separation. As a further precaution, all user accounts are audited at least quarterly, and any inactive user accounts are revoked.

3.2. Access Management

Botsify Inc. adheres to the principle of least privilege, and every action attempted by a user account is subject to access control checks.

Role-based Access Control

Botsify Inc. employs a role-based access control (RBAC) model utilizing Microsoft-supplied facilities such as organizational units, user accounts, user groups, and sharing controls where ever possible and practicable.

Web Browsers and Extensions

Botsify Inc. may require use of a specified web browser(s) for normal business use and for access to corporate data such as email. For certain specified roles such as software development and web design, job activities beyond those mentioned above necessitate the use of a variety of browsers, and these roles may do so as needed for those activities.

Any browser that is allowed to access corporate data such as email is subject to a whitelist-based restriction on which browser extensions can be installed.

Administrative Access

Access to administrative operations is strictly limited to security team members and further restricted still as a function of tenure and the principle of least privilege.

Regular Review

Access control policies are reviewed regularly with the goal of reducing or refining access whenever possible. Changes in job function by personnel trigger an access review as well.

3.3. Termination

Upon termination of personnel, whether voluntary or involuntary, the security team will follow Botsify Inc.' personnel exit procedure, which includes revocation of the associated user account and reclamation of company-owned devices, office keys or access cards, and all other corporate equipment and property prior to the final day of employment.

4. Provenance of Technology

How does Botsify Inc. build, adopt, configure, and maintain technology to fulfill its security intentions?

4.1. Software Development

Botsify Inc. and development partners, stores source code and configuration files in private Git repositories. The security and development teams conduct code reviews and execute a static code analysis tool on every code commit. Reviewers shall check for compliance with Botsify Inc.' conventions and style, potential bugs, potential performance issues, and that the commit is bound to only its intended purpose.

Security reviews shall be conducted on every code commit to security-sensitive modules. Such modules include those that pertain directly to authentication, authorization, access control, auditing, and encryption.

All major pieces of incorporated open source software libraries and tools shall be reviewed for robustness, stability, performance, security, and maintainability.

The security and development teams shall establish and adhere to a formal software release process.

Sensitive data which does not need to be decrypted (e.g. passwords) is salted and hashed using approved functions.

Sensitive data which must be decrypted (e.g. tokens) must use an approved encryption provider..

4.2. Configuration and Change Management

The Botsify Inc. security and development teams shall document the configuration of all adopted systems and services, whether hosted by Botsify Inc. or are third party hosted. Industry best practices and vendor-specific guidance shall be identified and incorporated into system configurations. All configurations shall be reviewed on at least an annual basis. Any changes to configurations must be approved by appointed individuals and documented in a timely fashion.

System configurations must address the following controls in a risk-based fashion and in accordance with the remainder of this policy:

- data-at-rest protection encryption
- data-in-transit protection of confidentiality, authenticity, and integrity for incoming and outgoing data
- data and file integrity
- malware detection and resolution
- capturing event logs
- authentication of administrative users
- access control enforcement
- removal or disabling of unnecessary software and configurations
- allocation of sufficient hardware resources to support loads that are expected at least twelve months into the future.
- production data is not used in development or test systems.

4.3. Third Party Services

For every third-party service or sub-processor that Botsify Inc. adopts, the compliance team shall review the service and vendor, on an annual basis, to gain assurance that their security posture is consistent with Botsify Inc.' for the type and sensitivity of data the service will store or access.

Botsify Inc. relies on Azure and Amazon Web Services (dependent on service) to satisfy specific security controls related to their respective data centres and services. For more information on Physical and Environmental Security, as well as the Logical Access and Security controls for AWS services, please see the AWS Security White Paper: https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

5. Data Classification and Processing

How does Botsify Inc. manage data classifications and data processing?

5.1. Data Classification

Botsify Inc. maintains the following Data Confidentiality Levels:

- Confidential - Information only available to specific roles within the organization. Data must be encrypted at rest and in transit. Access to data requires 2FA/MFA.

- Restricted - Access restricted to specific roles within the organization and authorized third parties. Data must be encrypted at rest and in transit. Access to data requires 2FA/MFA.

- Internal - Information is available to all employees and authorized third parties. Data must be encrypted at rest and in transit.

- Public - Information is available to the public.

Data Confidentiality is determined by:

- The value of the information, based on impacts identified during the risk assessment process.

- Sensitivity and criticality of the information, based on the highest risk calculated for each data item during the risk assessment.

- Policy, legal, regulatory, and contractual obligations.

Additionally, data may be separated into data type classifications to enforce processing rules for client data. For each data class, the Botsify Inc. security and development teams may provision and dedicate specific information systems in Azure or Amazon Web Services to store and process data of that class, and only data of that class, unless otherwise explicitly stated. For all classes of client data, data must be encrypted at rest and in transit. Corresponding systems may store and process data items needed to keep each client's data properly segmented, such as Botsify Inc. client identifiers.

Client User Account Data - This is data pertaining to login accounts for the client web interfaces, used by Botsify Inc. support agents. User account credentials shall be hashed in such a manner that the plaintext passwords cannot be recovered.

Client Contact Data - This is contact data about Botsify Inc. clients and support/account agents.

Client Preferences Data - This is data pertaining to the client-specific preferences and configurations of the Botsify Inc. service made by support agents.

Client Event Transaction Metadata - This is metadata about transactions conducted on all other classes of client data. This includes client organization and user identifiers, standard syslog data pertaining to client users, and instances of Client Contact Data and Client Preferences Data.

Client Contact Data, Client Preferences Data, and Client Event Transaction Metadata may be stored and processed in systems hosted in environments other than Amazon Web Services, as approved by the security team.

Client Customer Data – this is data that is specific to a client setup and possible integration into their own services. This data would be processed across our services and would be encrypted in transit, in process and at rest if applicable. This is bespoke to each client and changes for the scope of the usage of a system or project.

Resources must maintain accurate data classification tagging policies for their entire lifecycle, including during decommissioning or when removed from service temporarily.

5.2. Botsify Inc. Employee Access to Client Data

Botsify Inc. employees/support personnel may access Client Data only under the following conditions.

- From managed devices.
- For the purpose of incident response, or client support.
- For no longer than is needed to fulfill the purpose of access.
- In an auditable manner.
- Client Data is not used in development or test systems.
- Product usage metadata may be utilized for analytics, performance monitoring, and service/feature improvement.

5.3. Client Access

Botsify Inc. provides web user interfaces (UIs), application programming interfaces (APIs), and data export facilities to provide clients access to their data.

5.4. Exceptional Cases

The security team in conjunction with executive management may approve emergency exceptions to any of the above rules, in response to security incidents, service outages, or significant changes to the Botsify Inc. operating environment, when it is deemed that such exceptions will benefit and protect the security and mission of Botsify Inc., Botsify Inc. clients, and visitors of Botsify Inc. clients' websites.

5.5. Data Encryption

Botsify Inc. protects all data in transit with TLS 1.2 and all data at rest with AES-256 encryption from Amazon KMS. Cryptographic keys are assigned to specific roles based on least privilege access and keys are automatically rotated yearly. Usage of keys is monitored and logged.

Resources must maintain data encryption at rest and in transit for their entire lifecycle, including during decommissioning or when removed from service temporarily.

5.6. Data Retention

Each client is responsible for the information they create, use, store, process and destroy.

On expiration of services, clients may instruct Botsify Inc. to delete all client data from Botsify Inc.' systems in accordance with applicable law as soon as reasonably practicable, unless applicable law or regulations require otherwise.

5.7. Data Sanitization and Secure Disposal

Botsify Inc. uses Amazon Web Services for all infrastructure. AWS provides the following guidance regarding their data lifecycle policies:

Media storage devices used to store client data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored client data is not removed from AWS control until it has been securely decommissioned.

6. Vulnerability and Incident Management

How does Botsify Inc. detect, and respond to vulnerabilities and security incidents?

6.1. Vulnerability Detection and Response

The Botsify Inc. security and development teams shall use all of the following measures to detect vulnerabilities that may arise in Botsify Inc.' information systems.

- Cross-checking vulnerability databases with all systems and software packages that support critical Botsify Inc. services.
- Automated source code scanners on every code commit.
- Code reviews on every security-sensitive code commit.
- Vulnerability scanning on Botsify Inc. services.
- Maintain a bug bounty program.
- Annual penetration testing with an independent provider.

The Botsify Inc. security team shall evaluate the severity of every detected vulnerability in terms of the likelihood and potential impact of an exploit, and shall develop mitigation strategies and schedules accordingly. Suitable mitigations include complete remediation or implementing compensating controls.

6.2. Incident Detection and Response

The Botsify Inc. security team maintains an internal Incident Response Policy which contains steps for preparation, identification, containment, investigation, eradication, recovery, and follow-up/postmortem.

The Botsify Inc. security team shall use all of the following measures to detect security incidents.

- Continuous monitoring of AWS network traffic and workloads for malicious or unauthorized activities.
- Continuous monitoring of logs to detect potentially malicious or unauthorized activity.
- Conduct reviews on the causes of any service outages.
- Respond to notices of potential incidents from employees, contractors, or external parties.

The Botsify Inc. security team shall make a determination of whether every indicator is representative of an actual security incident. The severity, scope, and root cause of every incident shall be evaluated, and every incident shall be resolved in a manner and timeframe commensurate with the severity and scope.

In the event that a data breach affecting a client has been detected, Botsify Inc. will maintain communication with the client about the severity, scope, root cause, and resolution of the breach and reporting to the ICO.

7. Business Continuity and Disaster Recovery

How will Botsify Inc. prevent and recover from events that could interfere with expected operations?

7.1 Availability and Resiliency

Botsify Inc. services shall be configured in such a manner so as to withstand long-term outages to individual servers. Botsify Inc. infrastructure and data is replicated within AWS ensure this level of availability.

7.2 Disaster Recovery

Botsify Inc. targets a Data Recovery Point Objective (RPO) of near-zero for at least 7 days, and up to 24 hours beyond 7 days.

Due to the distributed nature of Botsify Inc. services, Recovery Time Objectives (RTO) are near-zero for geographic disasters. RTO for systemic disasters involving data recovery is targeted at 6 hours.

Botsify Inc. tests backup and recovery processes on at least a monthly basis

7.3 Business Continuity

Business Risk Assessment and Business Impact Analysis

Botsify Inc.' risk assessment will include business risk assessment and business impact analysis for each Key Business System that is used by the organization. The outcome of ongoing risk assessments will update or create recovery plans for Key Business Systems and update prioritization of systems compared to other key systems.

Distribution, Relocation, and Remote Work

Botsify Inc. prioritizes policies, tools, and equipment which enables independent, distributed remote work for all staff if emergencies or disasters strike. If the organization's primary work site is unavailable, staff can work from home or an alternate work site shall be designated by management.

Notification and Communication

Botsify Inc. has established internal communications using secure, distributed providers using industry standard security protocols. Staff and management will be notified via existing channels during any emergency event, or when any data recovery plan is initiated or deactivated.