Brandlive 2024 Security Policies

Table of Contents

Brandlive Information Security Policy

Document Version Control
Owner: Brandlive Security
Update Frequency: Annual
Document Version Control

Document Title:	**Information Security Policy**
Document Version	20230830.V1.4
Revision Number	1.4
Revision Date	20230821
Prepared by:	Brandlive Security
Authorized by:	Risk Management Committee

Revision History

Version	**Date**	**Author**	**Description**
1.0	04/27/18	Engineering Lead	Original Document
1.1	04/27/18	People Team	Physical and Environmental Updates
1.2	05/11/18	Engineering Lead	BCDR Update
1.3	02/01/21	Risk Management	Annual Update
20230523.V1.4	20232305	Brandlive Security	Annual Update
20230830.V1.4	20230830	Risk Management Committee	Approved

Purpose

The Information Security Policy aims to establish a program that protects the confidentiality, integrity, and availability of information assets at Brandlive. The policy defines the security program (“Program”) as well as minimum security controls. The Program's objectives include managing security risks within an established appetite, compliance with applicable laws and regulations, and establishing controls important to or required by Brandlive customer relationships.

Scope

This policy applies across all Brandlive information systems, including its employees, contractors, technology, products, and services.

Overview

The information security policy establishes high-level security objectives that leadership and the Risk Management Committee deem critical to maintaining confidentiality, integrity, and availability to Brandlive Information Systems. This policy sets forth domains and criteria each domain must address and maintain controls for. Each domain

shall have a supporting internal policy, standard, framework, or handbook addressing domain criteria.

Policy Alignment with External Standards

This policy applies across all Brandlive information systems, including its employees, contractors, and subsidiaries.

Standard	Alignment to the Security Policy
American Institute of Certified Public Accountants (AICPA) Trust Service Principles	Brandlive selects key controls for the Program, and documents them in the Control Framework. The controls in the Security and Availability trust principles from AICPA are used as a baseline to verify that no necessary controls have been omitted. In some cases, based on product, applicable HiTrust controls may be added to the scope of the AICPA audits.
National Institute of Standards and Technology (NIST)	Brandlive selects key controls for the Program, and documents them in the Control Framework. The controls within NIST are used for guidance to establish a baseline for handling data. Additionally, these controls ensure Brandlive information systems are implemented and operating according to industry standards.
Center for Internet Security (CIS),	Brandlive selects key configuration standards and documents them in the Control Framework. The controls within CIS are used for guidance to establish a baseline for configuring information systems.

Monitoring and Enforcement

Brandlive periodically monitors adherence to this Policy to help ensure compliance with applicable laws, requirements, and contractual agreements applying to Client and customer Data.

Penalties for failing to comply with Brandlive's Policies and Procedures could lead to disciplinary and/or enforcement actions against individuals and sanctions brought against Brandlive. Enforcement actions could include civil and/or criminal charges brought against violators depending on the seriousness of the offense.

Management Commitment

Brandlive's management is committed to and takes responsibility for implementing appropriate technical and organizational safeguards to ensure the protection of sensitive information (including personally identifiable information (PII)). Brandlive is also committed to demonstrating that any processing of sensitive information (including PII) is in compliance with all applicable regulations. Implemented measures will be reviewed and updated as necessary.

Roles and Responsibilities

Management

Management must demonstrate commitment and leadership over Brandlive's security and privacy management systems by ensuring the following:

- Security and privacy policies and objectives are in alignment with Brandlive's strategic direction;
- Security and privacy requirements are integrated into Brandlive's processes;
- Security and privacy resources are available;
- Security and privacy importance is communicated to and followed by Employees, third parties, and both internal/external stakeholders;
- Intended outcomes of the security and privacy programs are achieved;
- Direct and support personnel contribute to the effectiveness of the security and privacy programs;
- Security and privacy programs are continuously improved;
- Other management roles are supported in demonstrating leadership applied to their areas of responsibilities;
- Responsibilities and authorities for the security and privacy programs are assigned and communicated; those responsible ensure the programs conform to regulatory or contractual requirements with reports of performance provided to management; and
- Adequate monitoring and enforcement of policies and procedures are established.

Privileged Users

Privileged users are employees with elevated access to systems (such as system administrators) or individuals with assigned roles or responsibilities related to security and privacy. Privileged users are required to abide by and understand their assigned responsibilities related to their elevated access rights along with their limitations in using these privileges. Privileged users must understand their obligations and liabilities in utilizing their privileges as well as ensure they abide by separation of duties related to security and privacy activities.

Employees

Employees are responsible to abide by and understand all Brandlive's policies and procedures related to security and privacy. Employees are required to read and sign an acknowledgement and will abide by these Policies and Procedures. Employees will be subject to disciplinary actions, up to and including termination, for failing to abide by these Policies and Procedures.

Third Parties

Third parties, such as external service providers, are responsible to abide by Brandlive's policies and procedures related to security and privacy. Third parties must sign agreements with Brandlive concerning their responsibilities for implementing safeguards

to protect the security and privacy of data provided by Brandlive. Third parties failing to abide by these security and privacy requirements may be subject to legal actions, including the termination of contract for services.

Security Organization and Management Policy

Security Roles and Responsibilities

Brandlive has an organizational structure that establishes, approves, implements, and monitors adherence to an Information Security Program through clear lines of authority and responsibilities.

Risk Committee

Brandlive has appointed a Risk Committee consisting of internal personnel. The Risk Committee has oversight responsibilities related to all elements of the risk management framework, which are detailed in the Risk Committee Charter.
Responsibilities include the following:

- Approving and monitoring adherence to this policy
- Ensuring data handling responsibilities are assigned, documented, and communicated
- Review of the annual risk assessment

The Risk Committee meets at least quarterly and maintains formal meeting minutes.

Personnel

The following personnel are responsible for overseeing and implementing security and data protection practices throughout Brandlive:

- **Leadership:** Responsibilities include providing overall direction, leadership, and support on methods and tools for secure storage, retention, and disposal of Confidential and Sensitive data.
- **Systems Administrators/DevOps/Data Engineers:** Responsibilities include implementing the baseline configuration standards for all in-scope system components as well as managing user access to Brandlive information systems that contain Confidential and Sensitive data.
- **End Users (Employees, Consultants):** Responsibilities include adhering to the organization's data protection policies, procedures, and practices and reporting instances of non-compliance to senior authorities, especially instances by other users.
- **Third Parties(includes Contractors and other Vendors):** Responsibilities include all those applicable to end users. In addition, vendors, contractors, and third parties are responsible for:
    - Avoiding any measure to alter such standards that protect customer data;
    - Completing due diligence and ongoing monitoring assessments per the requirements set forth in the Third Party Risk Management Program; and
    - Immediately notifying Brandlive of any policy violations involving customer data.

Every end user and vendor is responsible for identifying and mitigating risks associated with the protection of Confidential information and must comply with all the policies within this Information Security Policy.

Policy Review

The Risk Committee is responsible for reviewing Brandlive's policies and procedures on at least an annual basis to ensure they remain accurate.

Data Classification

Data processed or controlled by Brandlive is outlined below to set for appropriate security and management of scoped information for employees, customers, and partners. The following is a list of data types with examples to communicate clarity and use of the data Brandlive holds.
Public: Information that is not confidential and can be made public without any implication for the organization. Such information is available to the public, employees, consultants, and contractors without authorization.
Internal: Information available to employees and authorized non-employees (consultants and contractors) possessing a need to know for business-related purposes.
Confidential: Information that is sensitive within Brandlive and is intended for use only by specified groups of employees. A breach of such information could cause reputational harm to the organization.
Customer: Information owned by the customer of which Brandlive is the custodian.
Personal Identifiable Information: information that can identify an individual alone or with other information. Examples of Personal Data include but are not limited to:

- Name, date of birth, social security number, or any other data that can lead to identifying an individual;
- Contact information such as mailing address, email address, phone number, and financial account numbers;
- Health or medical information;
- Information contained in employee files, including employment history, evaluations;
- Information collected during the application and hiring process; and
- Information related to employee benefits, such as dependent, beneficiaries, and insurance policy information

Policies

The following policies are intended to provide high-level direction and guidance from the risk management committee. Internal standards, procedures, and programs shall follow and be modified according to industry standards and best practices.

Risk Management

Brandlive shall design a risk assessment program. The program shall include criteria for managing risks through the risk management lifecycle.
The program will include but not be limited to the following activities.

- Planning
- Risk Assessment
- Risk Treatment
- Internal Audit
- Monitoring and Reporting

People Security

Brandlive shall implement personnel security controls as well as an Employee Handbook to guide security objectives and personnel expectations for managing risk from personnel screening, onboarding, termination, transfer, and management. The policy shall implement security best practices with regard to personnel processes and events.
The associated policies related to personnel security shall contain, but not be limited to the following organizational objectives:

- Require confidentiality agreements for all employees and contractors.
- Requirements for personnel screening shall be defined.
- Documented role and responsibilities.
- Security awareness and privacy training program, including role-based training and maintenance of records.
- Maintain onboarding, offboarding, and transfer procedures.
- Periodic performance assessments for personnel.

Access Control

Brandlive shall ensure that only authorized individuals can access Brandlive information systems and data. Access controls will prevent access to scoped information systems from unauthorized individuals.
The Access Control standards shall include but not be limited to:

- Account Management
- Least Privilege
- Access Enforcement
- Unsuccessful Login
- Remote Access

Third-Party Risk Management

Brandlive shall establish a third-party risk management program for all third parties to be reviewed before completing procurement activities. The third-party risk management program shall be implemented to help protect Brandlive from supply chain risks and help monitor ongoing remediation activities from suppliers. The third-party risk management program shall include but not be limited to:

- Rating third parties based on respective criticality
- Risk assessment methodology
- Due diligence and assurance requirements
- Acceptance criteria
- Ongoing monitoring

Business Continuity and Disaster Recovery

Brandlive shall establish a Business Continuity and Disaster Recovery program to ensure measures are taken to contribute to the commitment of availability and the continued offering of Brandlive services.
The Business Continuity and Disaster Recovery program shall include but not be limited to:

- Contingency Planning
- Contingency Planning Training
- Contingency Planning Testing
- Expectations for Backups

Change Management

Brandlive shall establish policies and procedures for handling changes to the organization's information system. Change management policies and controls shall help mitigate insider threats, malicious software from being introduced to Brandlive information systems and ensure appropriate testing before modifying scoped systems.
Change Management policy shall include but not be limited to:

- Criteria for changes
- Documentation expectations
- Types of changes
- Implementation of changes

Configuration Management

Brandlive shall establish and maintain policies and procedures for configuring scoped information systems. Configuration management policies and controls shall enable hardening practices and to enable security across Brandlive systems. Configuration Management policies and procedures shall include but not be limited to:

- Expectations for appropriate change control
- Impact analyses
- Baseline configurations
- Least functionality
- Asset inventory
- Configuration management plan
- Usage Restrictions

Incident Response

Brandlive shall establish an incident response program that maintains guidelines and procedures for responding to events that impact the confidentiality, integrity, and availability of the Brandlive information systems. Incident response functions shall enable team members to respond to events and incidents in a timely manner and follow necessary procedures for resolving incidents. The incident response policy and procedures shall include, but not be limited to:

- Definitions of an incident
- How to report an incident

- Assessment and containment guidance
- Recovery activities and guidelines
- Analysis
- Law enforcement contacts

System Development Life Cycle

Brandlive shall maintain a System Development Life Cycle to provide a consistent methodology for the development of software systems, involving stages of planning, analysis, design, development, testing, deployment, and maintenance. The system development policy shall include but not be limited to:

- System development life cycle guidance
- Use of data
- Use of external systems and services

System and Network Protection

Brandlive shall maintain a system and network protection policy that outlines expectations and guidelines for protecting organizational information systems. The system and network protection policy shall enable functions to protect data and systems from malicious behaviors. They shall include but not be limited to:

- Boundary protection and firewalls
- Host-based protections
- Encryption in transit
- Encryption at rest
- Cryptographic key management
- Cryptographic protections

System Integrity

Brandlive shall maintain a system integrity policy that outlines expectations for maintaining system integrity for organization information systems. The system integrity policy shall provide guidance and expectations on maintaining system security posture and monitoring and preventing malicious activities. The system integrity policy shall include but not be limited to.

- Flaw remediation and patch management
- Malware and endpoint protections
- Security alerts, advisories, and directives
- Data handling, retention, and disposal

Awareness and Training

Brandlive shall maintain and implement an awareness and training policy that will outline expectations for training and security awareness within the organization. Awareness and training shall encourage and enable a security-minded organization that will help prevent, detect, and respond to security-related events. The awareness and training policy shall include but not be limited to:

- Security awareness and privacy training

- Role-based training
- Maintaining security training records

Vulnerability and Patch Management

Brandlive shall maintain and implement policies and procedures for vulnerability and patch management practices. Vulnerability and patch management programs shall be maintained to reduce and respond to weaknesses and vulnerabilities within organization information systems. The vulnerability and patch management policy shall include but not be limited to:

- Patching systems
- Vulnerability scanning
- Vulnerability reporting

The remaining policies are confidential to Brandlive and can be accessed by reaching out to security@brandlive.com after completion of NDA.