BLOOMIN' BRANDS, INC.
INFORMATION TECHNOLOGY SECURITY POLICY

I. APPLICABILITY AND PURPOSE

This Information Security Policy ("Policy") establishes the components of the Information Security Program ("ISP") for Bloomin' Brands, Inc. ("BBI" or "Company").

A. General Application

The Policy applies to all Company Employees, Independent Contractors, Vendors, and Visitors who access the BBI Environment, which includes Electronic Devices, Network(s), Transmissions or Communication Systems, Computer Systems, Information Resources or Data, and physical locations and or premises. This Policy is subject to local jurisdiction laws and regulations and is supplemental to such laws and regulations where this Policy is inconsistent.

B. Specific Application

Sections I – III of this policy are applicable to all BBI Employees, Vendors, and Visitors. Section IV is applicable to Information Technology Employees only.

All BBI Employees are required to acknowledge that they have read, understood, and agree to abide by this Policy, as applicable, on an annual basis.

C. Purpose

This Policy is designed to:

- ensure that the Company is compliant with all applicable laws and regulations;
- ensure the security of Information Resources;
- protect against any anticipated threats or hazards to the security or integrity of data;
- protect against unauthorized access to or use of data in a manner that creates a substantial risk of identity theft or fraud; and
- define acceptable behaviors, promote higher standards and practices, and establish a framework for responsibilities.

II. DEFINITIONS

- **BBI Environment –** Encompasses all electronic Devices, Network(s), transmissions/communication systems, computer systems, Information Resources or data, and physical locations or premises owned by the Company.

- **Critical Systems –** Any system or application that processes or stores Confidential Data.

- **Confidential Data –** Critically sensitive data, as further defined in the *Data Security, Classification, and Retention Policy (Policy#IT04)*, which requires always the highest security protection; access to such data is limited and very strictly defined and controlled by *Policy #IT04.*

- **Corporate Data –** Internal data, as further identified and defined in the *Data Security, Classification and Retention Policy (Policy#IT04),* which is usually intended for Company use only and requires a heightened level of security, per *Policy #IT04*.

- **Device(s) –** Any electronic hardware owned by the Company, including Network(s), transmissions/communication, computer systems, resources, information, physical locations, premises and entities and data owned by the Company.

- **Guest Network** - A wireless (*a/k/a "Wi-Fi"*) router feature that is designed to allow users to easily grant "Visitor" access to a wireless internet connection.

- **Incident -** An event (e.g., a violation of Company policy) including a Security Breach which threatens the safety or security of the BBI Environment.

- **Information Resource(s)** - Corporate Data, Confidential Data, or Public Data.

- **Information Security Program ("ISP") –** Includes all information security policies, controls and dedicated resources. The goal of the program is to maintain the confidentiality, integrity and availability of all data and systems for the Company.

- **Network -** A collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.

- **Personal Device(s) –** Any electronic hardware or software not owned by the Company, as further defined the Company's *IT Hardware-Mobile Devices Policy (Policy #SC02).*

- **Personally Identifiable Data –** Information that can be used on its own or with other information to identify, contact, or locate a person, or to identify an individual in context.

- **Risk Assessment –** An analysis of the risks associated with permitting the activity/security requested.

- **Vendor** - Any third party doing business with Company, including suppliers of services and product.

- **Virtual Private Network ("VPN") -** A Network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the BBI Environment.

III. POLICY

A. Physical Security

The physical security requirements below define the minimum acceptable practices for security of the Company's electronic equipment (including the information contained in the equipment).

1. **Security measures.** The following physical protective measures must be followed:
   a) unauthorized physical access to the BBI Environment is strictly prohibited;
   b) where applicable, the Company will use tracking technologies to secure the BBI Environment;
   c) all electronic Devices must be secured with a password when not attended (e.g., lock your computer when not at your desk; personal electronic Devices or company issued electronic Devices must be password protected);
   d) Employees must take all necessary precaution to protect all parts of the BBI Environment on and off Company premises; and
   e) all Employees, Vendors, and contractors must immediately report any physical security violations or suspicious activity to Information Technology ("IT") Support.

2. **Access to physical Network.** Publicly accessible areas must not have physical access to the Network.

3. **Physical Access to BBI Environment.** Unauthorized access to BBI Environment or sensitive areas, including data centers is prohibited. Access to these areas must only be granted for work or engagement purposes only,

<u>Note</u>: Any external media, systems, Devices, or paper records (e.g., manual credit card slips, order forms, employee applications containing Company Confidential or Corporate Data must be physically secured at all times, and periodically inventoried. Electronic Devices can be secured by being locked in a secure room, cabinet, or equivalent, which access is restricted only to the necessary personnel.

B. Access, Authentication and Accountability

Unauthorized access to the BBI Environment is strictly prohibited. Access to the BBI Environment must be approved by the appropriate BBI authority. The BBI Environment is to be used only by Company Employees and Company authorized personnel. Access must be granted in accordance with BBI access request procedures and standards.

C. Passwords

Passwords must not be written down. They must not be disseminated, dissected, passed on or shared through any means.

1. **Password Complexity Requirements** - Passwords must:
   a) not contain any variation or derivation of the account name;
   b) not be words in any language, slang or jargon (i.e., the password should not be one that can be found in any dictionary);
   c) all passwords must contain upper and lower case alphabetic characters (*A-Z*, *a-z)*, numbers (*0-9*), and may also contain special characters (~` !@#$%^&*><\+-=_);
   d) all passwords must be at least eight characters in length; and
   e) BBI Environment passwords must not be the same password as used on other external systems or services.

2. Passwords are classified as Confidential Data and must follow the requirements outlined within Policy #IT04.

3. If an account or password is suspected to have been compromised; report the Incident to IT Support (BBI Support), and change all applicable passwords immediately.

D. Messaging and Communications

Employees must not use any type messaging technologies, such as email, instant messaging, and chat to send or receive Confidential Data. Employees must adhere to policy and guidelines set forth in the *Electronic Communications and Internet Use Policy (Policy #LG01).*

E. Information Ownership

Any Company Confidential or Corporate Data created in the BBI Environment which is destroyed within, entering or leaving through electronic or any other means is considered Company property. All data that is composed, transmitted, and/or received by the Company computer systems or Devices may also be considered Company property. Therefore, such data is subjected to full disclosure and audit, when required.

F. Personal Electronic Devices

A personal electronic Device may only interact with the BBI Environment if it is connected via one of the following; the Guest Network, remote VPN, or the outlook web client by Connecting a personal electronic Device into the BBI Environment, Employees, visitors, and Vendors agree that such personal electronic Device is subject to at will disclosure and may be the subject of seizure, inspection, and audit without prior notice. Inspection and audit will be performed by an authorized representative of the Company with Legal Department approval.

G. Visitors

Visitors will be provided access to the Guest Network which is isolated from all other Company owned systems. Visitors must comply with all physical access policies and procedures when on BBI premises.

H. Tracking and Monitoring

All Network traffic traversing the BBI Environment is subject to monitoring for the purpose of detecting and mitigating any Network threats and Policy violations. The Company monitors all transmissions/communications on all electronic Devices including personal electronic Devices that are in the BBI Environment.

I. Waiver

Requests for waiver to this Policy may be requested by Directors and above by completing a waiver request form signed by their departmental Vice President and submitted to the Global Chief Information Security Officer ("CISO") for review and approval consideration.

J. Enforcement

Any employee who violates this Policy may be subject to disciplinary action, up to and including termination of employment. This Policy will be enforced in accordance with human resources policies and procedures.

K. Information Security Awareness Training

Employees must complete the Information Security Awareness training program upon hire, and annually thereafter.

L. Vendor Management

A Risk Assessment and contract review must be performed by the Global Information Security ('GIS') for any Vendor that stores, transmits or processes data classified as Company Confidential or Corporate. At the discretion of GIS, additional Risk Assessments may be performed on the associated Vendor and all Vendor contracts must stipulate the Company's right to audit the Vendor's IT security controls. No Vendor that stores, transmits or processes Company Confidential or Corporate Data and/or accesses the BBI Network is allowed to transact with BBI without the completion of said Risk Assessment and direct approval from GIS.

M. Remote Access

1. Remote access to the BBI Environment shall be permitted only upon authentication of authorized Employees, Vendors, and Visitors.

2. All remote access sessions are held to the same policies and standards as defined in this Policy.

3. Two-factor authentication is required for any remote access session via VPN to any system or Device that is part of the BBI Environment.

N. Accountability

All individual access to the BBI Environment must be logged in a manner acceptable to Global Information Security. Critical system access logs are considered Corporate Data and must be retained according to *Policy #IT04***.**

O. Computer Security Controls

The computer security controls deployed to various Devices within the BBI Environment will be configured in accordance to security best practices, including anti-virus software. Employees, Vendors, and Visitors must not alter or disable the computer security controls for any reason without prior written permission from the CISO.

P. BBI Wireless Infrastructure

The BBI wireless infrastructure is for BBI business purposes only, with exception to occasional and reasonable personal use. Vendors, contractors, visitors and guests must not tamper with any BBI wireless infrastructure. Guest wireless Networks may be used where available and authorized.

Q. Usage Policy

Critical technologies are all electronic Devices, Networks, computer systems, applications, or databases that transmit, process, or store Confidential Data. Only authorized Employees, Vendors, and Visitors may access these systems using only approved authentication mechanism in accordance with the Access Authentication and Accountability Standards undefined. Employees, Vendors, and Visitors must not alter, replace, physically or logically move these technologies without prior authorization. Critical technologies must be used and protected in accordance with this Policy; IS published standards, procedures, and guidelines; and any applicable laws and regulations.

R. Information Security Incident Management

The Company must implement management controls and standards that result in a consistent and effective approach for addressing Incidents, including the collection of evidence related to the Incident as appropriate. Employees must report any observed or suspected Incidents; provide for Incident mitigation and remediation.

S. Compliance

The Company must safeguard all information assets and Information Resources through the implementation of the information security requirements found in this Policy, and in accordance with any relevant legislative, regulatory, and contractual guidelines and obligations.

IV. INFORMATION TECHNOLOGY EMPLOYEES ONLY

In addition to section three above, IT Employees are responsible for the following section.

A. Network Vulnerability Management and Penetration Testing Program

1. GIS must establish a vulnerability risk ranking program which will be used to identify, report, and prioritize all information security vulnerabilities in the BBI Environment. GIS will be responsible for managing the tools used for vulnerability and penetration scanning.

2. Penetration testing will be used to test all Critical Systems hosting, processing or transmitting Confidential Data, and their ability to withstand simulated attacks and identify other security gaps not identified by the vulnerability scans.

B. Hardening Standards

Any system or Device storing, processing, or transmitting any Confidential Data or Corporate Data or otherwise is part of the network segment which contains such Devices will be considered high risk and must adhere to BBI system hardening standards.

C. Application Security

All IT applications or systems whether owned and operated by BBI or hosted by 3rd party will be subject to a Risk Assessment conducted by GIS, in order to define the level of security required for the software or infrastructure.

D. Change Management

All production changes presenting any impact to the BBI Environment will follow the Company's change management process and in accordance to the *Change Management Policy (Policy #IT05).*

E. Information Technology projects and System Development Life Cycle ("SDLC")

The Company must ensure that information security is an integral component of all IT initiatives. Therefore, information security specifications and requirements must be considered at all phases of the SDLC, including application or system decommission. No IT initiative or project is allowed to be started without a completed review and approval by the GIS. Any requirements stipulated by GIS must be fully adhered to and all projects must validate compliance to such security controls. At the end of each project phase where security controls are stipulated, the project must receive GIS security certification before being placed into production. Only the Chief Information Officer or the Global Chief Information Security Officer (CISO) can waive such requirements.

F. Disaster Recovery Planning

The Company must document, implement, and annually test disaster recovery plans, including the testing of all appropriate IT security provisions to minimize impact to systems or processes from the effects of major failures of IT resources or disasters.

G. Information Security Roles and Responsibilities

1. The Company has designated the Global Chief Information Security Officer ("CISO") and assigned the following responsibilities:

   a) documentation, implementation, and maintenance of this Policy;
   b) training Employees, including conducting an annual training session on the elements of this Policy for all Employees, Vendors, and independent contractors who have access to BBI Environment;
   c) regular testing and auditing of this Policy's safeguards;
   d) evaluating the ability of Vendors to implement and maintain adequate security safeguards for the protection of Confidential Data and requiring such Vendors to implement and maintain appropriate security safeguards or protections;
   e) reviewing the scope of the security safeguards in this Policy at least annually or sooner, if there are material changes in the Company's business practices that may implicate the security or integrity of records containing Confidential Data; and
   f) periodic reporting on Policy compliance to the Company Executive Leadership Team.

2. The Global Information Security Team ("GIS") has been designated by the CISO. GIS shall design, manage, monitor, and operate Company security systems and the following responsibilities:

   a) establish, document, and distribute security policies and procedures;
   b) attend specialized security training periodically;
   c) monitor and analyze security alerts and information, and distribute to appropriate personnel;
   d) establish, document, and distribute security Incident response and escalation procedures to ensure timely and effective handling of all Incidents;
   e) administer user account and authentication management, including additions, deletions, and modifications; and
   f) monitor and control all access to Confidential Data; and provide security guidance to the Company by ensuring that any new processes, systems, and or applications are designed, developed, and managed to meet predefined security safeguards.

Appendix A - Policy Management

This Policy will be reviewed and updated on an annual basis to reflect any business, regulatory, or technology changes. The Policy is maintained and kept in sync with the growth of the Company and any other BBI Environment changes.

The policies listed below work in conjunction with this Policy to establish the Company's overall IT Security program:

1. *Electronic Communications & Internet Access Policy (Policy #LG01)*
2. *Data Security, Classification and Retention Policy (Policy # IT04)*
3. *Disaster Recovery Management Policy* (*Policy # IT03)*
4. *IT Hardware – Mobile Devices Policy (Policy #SC02)*
5. *Change Management Policy (Policy #IT05)*