Colony Brands, Inc. and Affiliates

Information Security Policy
(Policy 44)

Version 2.3

CONFIDENTIAL INFORMATION

This document is the property of Colony Brands Inc.; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Colony Brands Inc.

Revision History

Changes	Approving Manager	Date
Initial Publication	Kim Markham	March 2009
First Revision to comply with PCI DSS v.1.2		
Second Revision to increase scope of sensitive data	Shawn Lewis	September 2010
Reworked language throughout Removed procedural material Changed version	Shawn Lewis	May 2014
Added Transmission of Data Section Added Authentication Section	Shawn Lewis	October 2014
Extensive edits to summarize policy	Parker Smith	September 25 2015
Updated based on feedback from Legal	Todd Tupper	November 25, 2015
Updated based on feedback	Todd Tupper	November 3, 2022

Table of Contents

1 INFORMATION SECURITY POLICY SCOPE

This document explains the information security requirements of Colony Brands, Inc., its subsidiaries and affiliated companies (individually or collectively, “Company”). Company management has committed to the security policy to protect information and resources utilized by Company in attaining its business goals. These requirements apply to all Company employees, contractors, consultants, or agents, and all of them are required to adhere to the policies herein.

The Company Security Official manages Company information security activities. The Company Security Official works closely with Company executives and managers involved in securing Company information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed.

Company resources, whether owned or contracted, will be configured to meet the requirements set forth in these policies. Agreements that involve a third party accessing or managing Company resources shall comply with all of the requirements specified in these policies.

These policies are detailed and executed in the *Information Security Procedures*. Users agreeing to this policy also agree to follow the procedures outlined within the *Information Security Procedures*.

2 ACCEPTABLE USE

All users of Company digital resources must agree to and comply with the *Acceptable Use of Information Technology Resources Policy* (Policy #44A).

Information technology resources must be utilized respectfully and as authorized and designed. While utilizing these resources, no user is authorized to engage in any activity that violates a policy or that would constitute as “illegal” activity under local, state, federal or international law.

Users shall not interfere with, disable, or circumvent any security process, or engage in any activity that disrupts productivity or services of Company system resources. Exceptions to Policy #44A require documented authorization of the VP of Human Resources and/or the Security Steering Committee.

3 DATA GOVERNANCE

All users must abide by the Company *Data Access and Protection Policy*. This policy requires all data to be designated an owner, classified to an appropriate level, and handed with safeguards specific to that data classification. The Data Governance program will be coordinated by the Security team but relies on the cooperation and education of all users.

4 INFORMATION SYSTEM CHANGE CONTROL

Information System changes must be properly managed to ensure information resources are protected against unauthorized modifications throughout a system’s life cycle.

Production Information Systems, communication systems, related operating system software, hardware, procedures, and business applications, whether developed internally or purchased, may be subject to a Change Management Process.

5 ACCESS CONTROL

Company will provide users with the resources needed in order to carry out their responsibilities in an effective and efficient manner. Access to system(s) and data will be limited to authorized individuals whose job responsibilities require it, as determined by an approval process.

When a user no longer requires data access or leaves Company for any reason, the user's access privileges must be revoked in a timely manner.

6 DATA RETENTION

All data, regardless of storage location, will be retained only as long as required for legal, regulatory, and business requirements. The specific retention length will be coordinated by the Company Security Official with guidance from the Data Owner, business unit, and Legal.

7 ELECTRONIC AND PAPER DATA DISPOSAL

CAUTION – PRIOR TO DESTRUCTION OF ANY INFORMATION (WHETHER STORED IN PHYSICAL OR DIGITIAL FORM), YOU ARE REQUIRED TO: 1) CONFIRM THE DESTRUCTION IS AUTHORIZED UNDER THE COMPANY *RECORDS MANAGEMENT AND RETENTION POLICY* (Policy #85); 2) CONFIRM THAT THE INFORMATION IS NOT SUBJECT TO A LEGAL HOLD; AND 3) OBTAIN WRITTEN INSTRUCTION ONLY FROM PERSONNEL AUTHORIZED TO DIRECT THE DESTRUCTION OF COMPANY RECORDS. If destruction is deemed to be required, all Company information, stored in either physical or digital form, MUST be rendered unrecoverable using approved destruction methods when no longer needed for legal, regulatory, or business requirements. Outsourced destruction of media containing company information must use a bonded Disposal Vendor that provides a *Certificate of Destruction*, unless otherwise covered by an approved vendor operational process.

8 PERIMETER NETWORK DEVICES

Firewall and router connectivity paths and services, whether managed by Company or by third parties, must be configured to block Company networks and systems from unauthorized usage. Public facing services should be accessible only from the Company demilitarized zone (DMZ).

9 SYSTEM CONFIGURATION

All servers and network devices on Company networks, whether managed by employees or by third parties, must be built and deployed in accordance with security, standardization, and change management processes.

Prior to deployment into the production environment, all machines must conform to *System Configuration Standards*.

10 VULNERABILITY IDENTIFICATION & SYSTEM UPDATES

The Company Security Official must be informed of information security issues and vulnerabilities applicable to Company computing resources as they are discovered.

Internal and external network vulnerability scans are needed at least quarterly and after any significant change in the network. Internal and external penetration tests at both the application and network layer must be performed annually or after any significant change in the network for PCI compliance. Intermediate penetration and vulnerability tests may be performed by internal staff approved by the Company Security Official.

All potential identified vulnerabilities will be inventoried and communicated to appropriate personnel for assessment and remediation. Follow-up scans must be performed to confirm compliance with Company security standards.

Software patches, hot-fixes and service packs that impact the security of systems identified must be installed on applicable systems within one month of vendor release.

11 REMOTE ACCESS

Remote access rights will only be granted to users through a formal approval process. Company approved technologies must be used to minimize cybersecurity risk.

It is the responsibility of employees with Remote Access privileges to ensure that unauthorized users are not allowed to access Company internal network.

If there is a need to allow external access to a vendor, consultant or contractor, a maintenance window must be approved and scheduled. Activities during maintenance must be monitored and logged.

12 MALWARE PREVENTION

All systems commonly affected by malicious software such as servers, workstations, smartphones, laptops, tablets, smartphones, and any electronic device on the Company network, whether managed by employees or by third parties, must have Company-approved malware protection software.

Anti-malware software must be configured to scan a minimum of once per week on all Company-owned devices. Anti-malware definitions must be updated at least daily. Systems will provide real-time detection alerting.

Removing or permanently disabling anti-malware protection is a direct violation of this policy.

13 BACKUPS

Information technology backups provide a means to restore the integrity of a resource in the event of a hardware/software failure or physical disaster and to provide a measure of protection against human error or malicious activity. Backups are not intended to serve as an archival copy or to meet records retention requirements.

The Company is responsible for the backup of data held in central systems. Users bear full responsibility for backing up data stored locally on Company or personal devices. When possible, users should utilize central systems to backup Company data from their devices.

The backup media for each critical system will be inventoried and secured.

If transferring a physical backup, only approved couriers may be used, and chain of custody must be documented.

14 DATA ENCRYPTION

Only Company approved encryption mechanisms should be used to protect Company data. Company's encryption requirements will be reviewed annually and published in the *Information Security Procedures*. All data encryption keys and key generating procedures must be stored in a secure manner with strong access controls.

Exporting of encryption technologies is restricted by the U.S. Government. Company users working in countries other than the United States should make themselves aware of the encryption technology laws of the country in which they work.

15 SECURE APPLICATION DEVELOPMENT

It is the responsibility of Company users to ensure that all installed software is properly licensed. The Company must ensure that users in their departments are properly informed of their responsibilities regarding legal use of software. Company has the responsibility to request the removal of software that does not comply with licensing agreements or copyright law, but it is the responsibility of the user to comply with licensing agreements and copyright law.

All systems must be hardened against unauthorized use or attack while providing availability for necessary services. Security must be considered throughout the application development life cycle, including design, development, implementation, maintenance, decommission and destruction.

16 INCIDENT RESPONSE

The Company Security Official conducts and leads the assessment, containment, eradication, and remediation of reported breaches of sensitive data, and coordinates forensic investigation of reported incidents of malware, illegal computer usage, cyber-crime, and fraud.

The Company Security Official will establish, document, and distribute an Incident Response Plan to ensure timely and effective handling of security incidents involving organizational resources. Company users with IT responsibilities are responsible for understanding and following the Company Incident Response Plan.

In the event of a security incident the Company Security Official shall trigger the Incident Response Team. External forensic resources will be engaged as needed. The Company Security Official will issue a Security Incident Summary Report to the Security Steering Committee and will assist with the preparation of notification letters to victims when appropriate.

Suspected and confirmed security incidents, their resolution steps, and their outcomes shall be documented by those directly involved. The Company Security Official will ensure that incidents are appropriately logged and archived.

17 EMPLOYEE IDENTIFICATION

When applicable, all users of Company system and network resources must comply with the *Physical Security Policy* (CSP300).

The Safety Department, in conjunction with Management, will determine what privileges are necessary for employees or users to perform their job functions and issue badges accordingly. Data and other security policies are considered when issuing physical access privileges.

Visitors entering any Company facility will be required to sign in at the designated reception area. Visitor badges are clearly distinguishable from assigned employee ID badges. In no case may a visitor ID badge permit unescorted access throughout any Company facilities, especially to physical areas that store sensitive data.

18 AUDIT & LOGGING

Automated audit trails must be implemented for all high-risk system components to reconstruct events. When possible, systems should use approved configuration templates when deploying systems.

Event logs must be collected in media that is difficult to alter and protected from unauthorized access. Audit logs need to provide the ability to link suspicious activity to a specific user and specific device when possible. The logs will be further protected by a file integrity monitoring (FIM) system that alerts Company upon unauthorized access.

Regular audits shall be conducted by designated Company employees. Findings indicating a security incident should be investigated immediately per the *Incident Response Procedure*.

19 SECURITY AWARENESS TRAINING

The Information Security Department maintains an Information Security Awareness Training program that provides users with regular training, supporting reference materials, and reminders to enable them to appropriately protect Company resources.

Users with access to confidential data must complete security training annually. Departments shall maintain appropriate documentation of attendance/completion of training where information security training is required by applicable industry or regulatory standards.

20 RISK MANAGEMENT

The Company Security Official is responsible for developing a process for conducting Risk Assessments for Company’s information technology resources. The results of the Risk Assessments will be used to determine security improvements resulting in reasonable and appropriate levels of risk acceptance and compliance of each system.

Results indicating an unacceptable level of risk shall be remediated as soon as possible, as determined by specific circumstances and the timelines decided collectively by the Company Security Official, CIO, Information Security Committee and Department Leaders. Results of all risk assessments shall be treated as confidential and secured appropriately.

21 PHYSICAL ACCESS

Access to areas such as data centers, computer rooms, communication closets and network equipment rooms will be restricted to authorized personnel only. Areas where Sensitive Data is stored or processed shall be restricted to authorized personnel and access to these areas shall be logged.

The *Physical Security Policy* (CSP300) provides physical security reporting and control measures that Company requires for each facility.

22 BUSINESS CONTINUNITY & DISASTER RECOVERY

The Business Continuity Plan (BCP) will be an action-based plan that addresses the recovery of critical systems and data following disruptive incidents.

The Disaster Recovery (DR) Plan addresses maintaining business processes and services in the event of a disaster and the eventual restoration of normal operations. The BCP and DR Plan will contain a documented process for annual review, testing, and revision. Annual testing of the BCP should include walkthrough, tabletop testing, live simulations, and data restoration procedures, when appropriate. The BCP will include measures necessary to protect sensitive data during emergency situations.

23 INTRUSION DETECTION

The Company will deploy intrusion detection and prevention (IDP) capabilities as part of defense-in-depth strategy to prevent, monitor and identify system intrusions or misuse.

Intrusion detection and prevention (IDP) capabilities shall include guidelines for monitoring and analyzing system logs, notifications, warnings, alerts, and audit logs. Company shall identify and train skilled personnel to maintain and review information technology security audit logs and intrusion prevention and detection system alerts on a regular basis to detect security incidents.

24 WIRELESS DEVICE COMMUNICATION

All wireless devices that connect to the Company's network or reside on the Company's site that provide wireless connectivity to endpoint devices including but not limited to laptops, desktops, tablets, smartphones, and any form of wireless device capable of transmitting packet data are subject to Company policies. The Company is sole owner of the unlicensed frequencies throughout our facilities. Unauthorized wireless devices will be disabled or removed from company property to prevent interference and safeguard Company resources.

Wireless devices utilizing Company wired infrastructure must meet acceptable standards to ensure only authenticated and authorized users connect to the Company network. Institutional data used by Company users and systems must not be exposed to unauthorized viewers.

25 EXCEPTIONS

Users must submit requests for any exception to this policy in writing to the Company Security Official for review. Exceptions to this policy are reviewed based on operational constraints, technical limitations, legal requirements, or other issues. Exemptions from this policy will be permitted only if formally approved in advance by the Company Security Official. Exceptions to this policy will be inventoried and reviewed regularly.

A valid business justification and risk assessment should exist for all deviations from security policy, procedures, and standards.

26 ENFORCEMENT & DISCIPLINE FOR A VIOLATION

For purposes of protecting the Company network and information technology resources, the Company may temporarily remove or block any system, device, or person suspected of violating this policy from any Company resources. Devices held in quarantine are temporarily owned by IT Security until cleared.

All reports of violations of this policy will be investigated. Violation may result in disciplinary action up to and including termination of employment. The Company reserves the right to take legal action where necessary against employees who engage in prohibited or unlawful conduct.