Taco Bell
Security & Acceptable Use Policy
ColCal

Franchise operators
proudly serving Taco Bell

These policies are required to be reviewed annually:

Name	Date of review	Changes
JHarmon	08/31/2012	Initial creation
RNeill	10/17/2012	Revision
RSmith	10/17/2014	Revision
BHendershot	12/28/2015	Revision
KBasinger	12/08/2016	Revision
KBasinger	03/10/2017	Revision
Kbasinger	02/20/2018	Revision

1 POLICY ROLES AND RESPONSIBILITIES

1.1 Policy Applicability
These policies apply to all full and part time employees of ColCal and any personnel contracted to perform function within the prosperities owned or managed by ColCal.

1.2 Chief Security Officer
The Controller is responsible for enforcement with Payment Card Industry (PCI) and other security regulations as needed by ColCal.

1.3 Information Security Department
This department is responsible for managing the security and compliance for ColCal.

1.4 System Administrators
Not applicable if using Taco Bell Supported Systems, that includes the certified Back Office, Point of Sale and Certified Broadband for connectivity.

1.5 Human Resources Department
This department is responsible for the staffing, any personnel issues including development, and conducting background checks for all new hires.

1.6 Users
Only authorized users that are current employees of ColCal or those contracted for a specific purpose.

2 PAPER AND ELECTRONIC MEDIA POLICIES

2.1 Policy Applicability
These policies apply to all full and part time employees of ColCal and any personnel contracted to perform function within the prosperities owned or managed by ColCal.

2.2 Storage
The storage of any payment card information in any format is strictly prohibited, any documentation that contains sensitive Personal Identifiable Information (PII) has to remain secured and only accessed by authorized personnel. Any electronic media that contains PCI or PII has to be secured.

2.2.1 Physical Security
All media that do or could contain PCI or PII information has to be physically secured when not in use. The physical security should be robust enough to stop a reasonable person for gaining access.

2.2.2 Hardcopy Media
This is any media that is not electronic that is human readable, this can be paper, plastic, or any other media that have, could or still do contain PCI or PII information.

2.2.3 Electronic Media
This is any media that is not human readable to include optical media, soft magnetic media, or hard drives that have, could or still do contain PCI or PII information.

2.3 Inventory
A documented inventory of all material that does or could contain PCI or PII information has to be maintained and secured in the home office of ColCal. This documentation should also contain the date of the disposal of the material.

2.4 Destruction
Any physical media (paper, optical media, soft magnetic media, or hard drives) that contained or could contain PCI or PII information have to be securely destroyed. This should be certified by either an approved destruction vendor or the Chief Security Officer or the individual serving in this capacity.

3 USAGE POLICY FOR CRITICAL TECHNOLOGIES

3.1 Policy Applicability
These policies apply to all full and part time employees of ColCal and any personnel contracted to perform function within the prosperities owned or managed by ColCal.

3.2 Approval
Approval for usage is passed from the Chief Security Officer to the managers of the individual units to determine who is authorized to access both the back office computer as well as the point of sale terminals.

3.3 Authentication
Each device must have a unique user access code assigned to the users. Users are prohibited from sharing or allowing the use by another individual their personal access codes for either the back office computer or point of sale equipment.

3.4 Device Inventory
The inventory of the critical devices is maintained in the home office as well as the implementation department of Taco Bell. These devices include the back office computers and the point of sale terminals.

3.5 Device Identification
The devices are identified by their position within the restaurant; the back office computer is in the office, the point of sale terminals are on the front counter or in the drive thru areas.

3.5.a Inspections of Secure Pay Terminals

All secure payment terminals will be inspected for signs of tampering or modification by the MIC at least once per day (ideally, during opening procedures). Secure payment terminals will be inspected following the procedures provided by Taco Bell. The MIC will record the results of the inspection on the tracking log.

3.5.b Verification of Payment Device Identification

All secure payment terminals will be checked to confirm the device has not been replaced without authorization. The MIC should check the exterior of the device for signs of replacement, including: presence of labels or other decals; unusual marks or other physical characteristics; and verification the serial number matches the records

3.5.c Preventing and Detecting Changes to Payment Terminals

All personnel and specifically store management should be aware of any changes that may made to payment terminals, specifically:

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not to install, replace, or return devices without verification.
- Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report all suspicious behavior to appropriate personnel (for example, RGM, area coach, franchise office, and/or Taco Bell Help Desk).
- Report tampering or substitution of devices.

3.6 Acceptable Use

The only acceptable use of the critical equipment if for the management, sale of products, and training of store personnel located within a particular restaurant and are an employee of ColCal or have been given authority for training by ColCal.

3.7 Permitted Locations

The only permitted location for critical equipment are in the restaurant the equipment is assigned, or in a secure spare parts storage facility as identified by ColCal.

3.8 Approved Products

The approved products are identified and maintained by Taco Bell. Only those products that have been identified by Taco Bell are allowed for use in the restaurants.

3.9 Session Disconnect

This is not applicable as ColCal does not have the ability to remotely connect to their critical systems.

3.10 Vendor Connections

All of these types of connection are managed by Taco Bell and fall under the service provider assessment for Taco Bell.

3.11 Cardholder Data Access
This is only allowed in a one card at a time situation for the payment of merchandise using approved point of sale equipment as provided by Taco Bell for use by ColCal.

3.12 Portable Devices
No portable devices shall be connected to the store network at any time for any reason.

4 EMPLOYEE IDENTIFICATION POLICY

4.1 Policy Applicability
These policies apply to all full and part time employees of ColCal and any personnel contracted to perform functions within the properties owned or managed by ColCal.

4.2 Employee Requirements
All employees are required to be in uniform when working per the Taco Bell Policy. Non-managerial employees are not allowed behind the counter of any restaurants when not working or out of uniform unless escorted by a manager.

4.3 Facilities
The facilities included are the home office and restaurants owned and operated by ColCal. Proper identification is required at all times while in the facilities that have PCI and or PII information.

4.4 Badge Assignment Procedure
Badges are not used by the Taco Bell Uniform policy.

4.4.1 New Badges
Badges are not used by the Taco Bell Uniform policy.

4.4.2 Visitor Badges
Visitor badges are not used, all visitors are escorted by the manager on duty and required to sign in the visitors log upon arrival and departure at all facilitates owned and operated by ColCal.

4.4.3 Changing Access
Access levels are not set at ColCal, restaurant employees are allowed in any facility owned and operated by ColCal.

4.4.4 Revoking Badges
Badges are not used by the Taco Bell Uniform policy.

5 THIRD PARTIES AND THIRD PARTY AGREEMENTS

5.1 Policy Applicability

These policies apply to all full and part time employees of ColCal and any personnel contracted to perform function within the prosperities owned or managed by ColCal.

5.2 Sharing of Cardholder Data

PCI or PII data can only be shared with approved service providers such as the acquiring banks or Taco Bell, providing they have a business need for such information.

6 PAYMENT CARDHOLDER DATA BREACH INCIDENT RESPONSE

6.1 *Scope of Cardholder Data Environment*

The scope of the cardholder data environment at Colcal includes only the secure payment devices. There are no other authorized methods of accepting card payments.

6.2 *Breaches of Secure Payment Devices*

Due to the scope of the cardholder data environment, any detected tampering or substitution of secure payment devices will be immediately reported to Colcal management and the appropriate help desk.

6.3 *Breaches of Cardholder Data*

By using the secure payment devices, Colcal does not have any cardholder data stored either electronically or in physical form (hard copy reports); nor does Colcal have access to the cardholder data before it is encrypted for transmission to the bank. Colcal will report any suspected breaches of the secure payment devices that could have exposed cardholder data to the appropriate help desk. "