SAMPLE LETTER

meritage HOSPITALITY GROUP

November 3, 2025

[Employee Name]
[Employee Address]

Re: Data Breach Notification

Dear [Employee]:

Inspired by Opportunity, LLC and Meritage Hospitality Group, Inc. (collectively, "Meritage"), are providing required notice of a security breach of a database containing your personal information, on July 8, 2025. Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below.

You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

- Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/
- Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 https://www.experian.com/freeze/center.html
- TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card,

military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

We regret that this incident occurred and any inconvenience it may have caused. IBO is providing you with access to Equifax – ID Watchdog identify theft prevention services at no charge for 24 months. To enroll in these services, please follow the instructions at this link: [INSERT CUSTOM LINK]. I am enclosing an explanatory brochure for your review. To obtain additional information, please contact me directly at mijohnson@mhgi.net, or (616) 608-9028.

Sincerely,

Miranda Johnson

Miranda Johnson
Director of Human Resources

idwatchdog® from Equifax

No one is immune to identity theft.

Better Protect What Matters Most.

Identity theft can affect anyone—from infants to seniors. Each generation has habits that savvy criminals know how to exploit—resulting in over $47 billion lost in the US to identity fraud in 2024[1]. Take action with award-winning ID Watchdog® identity theft protection.

Greater Peace of Mind

With ID Watchdog® as an employee benefit, you have a more convenient and affordable way to help better protect and monitor your identity. You'll be alerted to potentially suspicious activity and enjoy greater peace of mind knowing you don't have to face identity theft alone.

javelin 2024 IDENTITY PROTECTION SERVICES PROVIDER SCORECARD BEST IN CLASS 2024

ID Watchdog® was awarded the **2024 Best in Class Identity Protection Service Provider**

Why Choose ID Watchdog?

Financial & Identity Fraud Protection

Put your trust into an award-winning identity theft protection service, recognized by Javelin Strategy & Research as a "Best in Class" leader for three consecutive cycles — we've built a reputation on excellence for our capabilities in detection, monitoring, alerting, and prevention.

Extensive Family Protection

We offer more features to help protect minors than any other provider. Our family plan helps you better protect your loved ones with personalized accounts for adult family members, family alert sharing, and exclusive features for children[2].

Personal Cyber Security

We want to empower you to navigate the digital world more safely. Our solution includes robust digital privacy and device security tools you can implement on your devices — helping to reduce the likelihood of cyber attacks, phishing, or other AI-powered scams.

Resolution & Insurance

We've made protecting you and your family from financial losses even easier — offering a financial safety net that makes sense for a broad array of situations to extend peace of mind. Even more, our team of resolution specialists are here to walk you through it, step by step.

Our US-based, customer care team is **here for you 24/7/365 at 866.513.1518.**

Learn more about this valuable benefit at **idwatchdog.com/myplan/xxxxxxxxx**

1 2025 Identity Fraud Study: Breaking Barriers to Innovation, Javelin Strategy & Research.
2 Refer to your employer or ID Watchdog® for family plan eligibility.

ID Watchdog® **Ultimate**

Powerful features for end-to-end support

Financial Protection

- Credit Report Lock[1]
- Blocked Inquiry Alerts
- 3-Bureau PreCheck[2]
  - *Encourages potential lenders to verify your identity before extending credit*
- Subprime Loan Block[3]
  - *Within the monitored lending network*
- Credit Reports & VantageScore® Credit Scores | 3-Bureau (Annually), 1-Bureau (Unlimited)
- Credit Score Tracker
- Credit Report Monitoring[4] | 3 Bureau
- Accelerated Credit Inquiry Alerts
- Telecom & Utility Alerts
- High-Risk Transaction Monitoring[3]
- Financial Accounts Monitoring
- Subprime Loan Monitoring[3]

Identity Fraud

- Dark Web Monitoring[5]
- AI-Powered Phishing & Malware Alerts
- Social Accounts Monitoring
- Public Records Monitoring
- USPS® Change of Address Monitoring
- National Provider ID Alerts
- Registered Sex Offender Reporting

Personal Cyber Security

- Digital Privacy Scans & Removal[6]
- Personal VPN with Threat Protection, Up to 10 devices at the same time
- Password Manager, Unlimited devices
- Device Security & Online Privacy Up to 5 devices, 10 with a Family Plan
  - Antivirus Protection
  - Mobile Scam Alerts
  - Browser & Phishing Protection
  - Missing & Stolen Device Tools
  - Network & Privacy Firewall
  - Webcam & Microphone
  - Cryptomining Protection NEW

Reimbursement & Support

- Personalized Identity Restoration, including Pre-Existing Conditions
- Online Resolution Tracker
- Identity Theft Insurance[7] Up to $5M (per adult)
  - Up to $2M Stolen Funds Reimbursement
  - Home Title Fraud
  - Cyber Extortion
  - Professional Identity Fraud
  - Deceased Family Member Fraud
  - Senior Family Coverage
  - Up to $500 Stolen Cash Replacement
- Lost Wallet Vault & Assistance
- Deceased Family Member Fraud Remediation (Family Plan only)
- Cyber Crime Coverage[8] NEW Up to $50k
  - Online Fraud & Scams
  - Cyber Extortion Response
  - Cyberbullying Expenses
- Credit Freeze Assistance
- Data Breach Notifications
- Solicitation Reduction
- Legal Care[9]
- Mobile App
- 24/7/365 Customer Care Center
- Online Chat NEW

Family Protection

- Family Alert Sharing
- Child Credit Lock
- Child Credit Monitoring
- Parental Controls Unlimited Devices
  - Online Activity Monitoring
  - Online Search & Content Control
  - Screen Time Management
  - Internet Time Reward System NEW
  - Geolocation Tracking & Alerts

NEW = Targeted to be available by Oct 2025*

1 Bureau = Equifax® | 3 Bureau = Equifax®, Experian®, TransUnion®

A child's identity can provide a blank slate for fraudsters

Help better protect your children from identity theft with features marked with this icon.

Special Employee Pricing	Per Month
Employee	$x.xx
Employee + Family	$x.xx

Take a step to help better protect your identity.

Enroll in this valuable benefit today.

What You Need to Know

The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore® uses Equifax® data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

(1)Locking your Equifax® credit report will prevent access to it by certain third parties. Locking your Equifax® credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax® credit report include: companies like ID Watchdog®, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state, and local government agencies; courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of pre-approved offers, visit optoutprescreen.com. (2)The 3-Bureau PreCheck feature is made available to consumers by Equifax® Information Services LLC and fulfilled on its behalf by Identity Rehab Corporation. (3)The monitored network does not cover all businesses or transactions. (4)Monitoring from TransUnion® and Experian® will take several days to begin. (5)There is no guarantee that ID Watchdog® is able to locate and scan all deep and dark websites where consumers' personal information is at risk of being traded. (6)There is no guarantee that we can detect or remove consumer personal information from all people search sites. (7)The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Review the Summary of Benefits (idwatchdog.com/terms/insurance). Coverage may not be available in all jurisdictions. (8)Cyber Crime Coverage is currently available to all customers residing in the United States, including U.S. territories and the District of Columbia, with the exception of residents of New York. ID Watchdog® is not a licensed insurance producer. Benefits under the Master Policy are issued and covered by HSB Specialty Insurance Company. Review the Summary of Benefits for further details and explanation. (idwatchdog.com/terms/cybercrimecoverage), (9)Gain access to a nationwide network of plan attorneys. Plan includes nine legal services at no additional charge (e.g., simple will) and discounted rates for other legal services. *May be subject to delay or change.

EQUIFAX

DESCRIPTION OF ID PROTECTION SERVICES

idwatchdog® from Equifax

No one is immune to identity theft.

Better Protect What Matters Most.

Identity theft can affect anyone—from infants to seniors. Each generation has habits that savvy criminals know how to exploit—resulting in over $47 billion lost in the US to identity fraud in 2024[1]. Take action with award-winning ID Watchdog® identity theft protection.

Greater Peace of Mind

With ID Watchdog® as an employee benefit, you have a more convenient and affordable way to help better protect and monitor your identity. You'll be alerted to potentially suspicious activity and enjoy greater peace of mind knowing you don't have to face identity theft alone.

javelin 2024 IDENTITY PROTECTION SERVICES PROVIDER SCORECARD BEST IN CLASS 2024

ID Watchdog® was awarded the **2024 Best in Class Identity Protection Service Provider**

Why Choose ID Watchdog?

Financial & Identity Fraud Protection

Put your trust into an award-winning identity theft protection service, recognized by Javelin Strategy & Research as a "Best in Class" leader for three consecutive cycles — we've built a reputation on excellence for our capabilities in detection, monitoring, alerting, and prevention.

Extensive Family Protection

We offer more features to help protect minors than any other provider. Our family plan helps you better protect your loved ones with personalized accounts for adult family members, family alert sharing, and exclusive features for children[2].

Personal Cyber Security

We want to empower you to navigate the digital world more safely. Our solution includes robust digital privacy and device security tools you can implement on your devices — helping to reduce the likelihood of cyber attacks, phishing, or other AI-powered scams.

Resolution & Insurance

We've made protecting you and your family from financial losses even easier — offering a financial safety net that makes sense for a broad array of situations to extend peace of mind. Even more, our team of resolution specialists are here to walk you through it, step by step.

Our US-based, customer care team is **here for you 24/7/365 at 866.513.1518.**

Learn more about this valuable benefit at **idwatchdog.com/myplan/xxxxxxxxx**

1 2025 Identity Fraud Study: Breaking Barriers to Innovation, Javelin Strategy & Research.
2 Refer to your employer or ID Watchdog® for family plan eligibility.

ID Watchdog® **Ultimate**

Powerful features for end-to-end support

Financial Protection

- Credit Report Lock[1]
- Blocked Inquiry Alerts
- 3-Bureau PreCheck[2]
  - *Encourages potential lenders to verify your identity before extending credit*
- Subprime Loan Block[3]
  - *Within the monitored lending network*
- Credit Reports & VantageScore® Credit Scores | 3-Bureau (Annually), 1-Bureau (Unlimited)
- Credit Score Tracker
- Credit Report Monitoring[4] | 3 Bureau
- Accelerated Credit Inquiry Alerts
- Telecom & Utility Alerts
- High-Risk Transaction Monitoring[3]
- Financial Accounts Monitoring
- Subprime Loan Monitoring[3]

Identity Fraud

- Dark Web Monitoring[5]
- AI-Powered Phishing & Malware Alerts
- Social Accounts Monitoring
- Public Records Monitoring
- USPS® Change of Address Monitoring
- National Provider ID Alerts
- Registered Sex Offender Reporting

Personal Cyber Security

- Digital Privacy Scans & Removal[6]
- Personal VPN with Threat Protection, Up to 10 devices at the same time
- Password Manager, Unlimited devices
- Device Security & Online Privacy Up to 5 devices, 10 with a Family Plan
  - Antivirus Protection
  - Mobile Scam Alerts
  - Browser & Phishing Protection
  - Missing & Stolen Device Tools
  - Network & Privacy Firewall
  - Webcam & Microphone
  - Cryptomining Protection NEW

Reimbursement & Support

- Personalized Identity Restoration, including Pre-Existing Conditions
- Online Resolution Tracker
- Identity Theft Insurance[7] Up to $5M (per adult)
  - Up to $2M Stolen Funds Reimbursement
  - Home Title Fraud
  - Cyber Extortion
  - Professional Identity Fraud
  - Deceased Family Member Fraud
  - Senior Family Coverage
  - Up to $500 Stolen Cash Replacement
- Lost Wallet Vault & Assistance
- Deceased Family Member Fraud Remediation (Family Plan only)
- Cyber Crime Coverage[8] NEW Up to $50k
  - Online Fraud & Scams
  - Cyber Extortion Response
  - Cyberbullying Expenses
- Credit Freeze Assistance
- Data Breach Notifications
- Solicitation Reduction
- Legal Care[9]
- Mobile App
- 24/7/365 Customer Care Center
- Online Chat NEW

Family Protection

- Family Alert Sharing
- Child Credit Lock
- Child Credit Monitoring
- Parental Controls Unlimited Devices
  - Online Activity Monitoring
  - Online Search & Content Control
  - Screen Time Management
  - Internet Time Reward System NEW
  - Geolocation Tracking & Alerts

NEW = Targeted to be available by Oct 2025*

1 Bureau = Equifax® | 3 Bureau = Equifax®, Experian®, TransUnion®

A child's identity can provide a blank slate for fraudsters

Help better protect your children from identity theft with features marked with this icon.

Special Employee Pricing	Per Month
Employee	$x.xx
Employee + Family	$x.xx

Take a step to help better protect your identity.

Enroll in this valuable benefit today.

What You Need to Know

The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore® uses Equifax® data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

(1)Locking your Equifax® credit report will prevent access to it by certain third parties. Locking your Equifax® credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax® credit report include: companies like ID Watchdog®, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state, and local government agencies; courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of pre-approved offers, visit optoutprescreen.com. (2)The 3-Bureau PreCheck feature is made available to consumers by Equifax® Information Services LLC and fulfilled on its behalf by Identity Rehab Corporation. (3)The monitored network does not cover all businesses or transactions. (4)Monitoring from TransUnion® and Experian® will take several days to begin. (5)There is no guarantee that ID Watchdog® is able to locate and scan all deep and dark websites where consumers' personal information is at risk of being traded. (6)There is no guarantee that we can detect or remove consumer personal information from all people search sites. (7)The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Review the Summary of Benefits (idwatchdog.com/terms/insurance). Coverage may not be available in all jurisdictions. (8)Cyber Crime Coverage is currently available to all customers residing in the United States, including U.S. territories and the District of Columbia, with the exception of residents of New York. ID Watchdog® is not a licensed insurance producer. Benefits under the Master Policy are issued and covered by HSB Specialty Insurance Company. Review the Summary of Benefits for further details and explanation. (idwatchdog.com/terms/cybercrimecoverage). (9)Gain access to a nationwide network of plan attorneys. Plan includes nine legal services at no additional charge (e.g., simple will) and discounted rates for other legal services. *May be subject to delay or change.

EQUIFAX

POLICIES AND PROCEDURES

Information & Cyber Policy

Effective Date: 2024
Policy Number: 06.005.01 (Consolidated)

1. Purpose

The purpose of this comprehensive Information Security Policy is to establish guidelines and standards to protect the organization's employees, assets, customer information, employee information, integrity, and reputation from potential security threats. These threats include:

- Compromise of confidentiality (unauthorized access or disclosure of information)
- Compromise of integrity (deliberate or accidental alteration of information)
- Compromise of availability (information unavailable when required)

2. Scope

Information and Cyber Security is addressed in this policy through the following data management processes:

- Data Classification & Handling
- Password Protection Standards
- Network Security
- Email and Internet Security
- Device Management
- Physical Security
- Incident Response
- Business Continuity and Disaster Recovery
- Data Encryption and PCI DSS Compliance
- Training and Accountability

This policy applies to:

- All Company employees and temporary workers at all locations
- Contractors working with Company information
- All hardware, software, communication equipment, and devices used for information processing
- Equipment connected to any Company domain or VLAN (hardwired, wireless, or cloud-based)
- Stand-alone equipment deployed at the Restaurant Service Center or remote locations

3. Data Classification and Handling

- **Introduction:** Data classification is fundamental to protecting the organization's information assets. By clearly defining different levels of sensitivity and establishing specific handling requirements for each level, we ensure that information receives appropriate protection while remaining accessible for legitimate business purposes. This framework helps prevent data breaches, maintains compliance with regulations, and protects both the company and customers' interests.

3.1 Classification Levels and Handling Procedures

3.1.1 Restricted Data

- Definition: Information that would cause severe damage to the organization if disclosed
- Examples: PCI data, personal health information, financial records, security infrastructure details
- Access Requirements:
  - Limited to specifically named individuals with documented approval
  - Annual review of access rights
  - Multi-factor authentication required for all access
  - Written approval from data owner required for any access changes
- Storage Requirements:
  - Must be encrypted at rest using approved encryption methods
  - Must be stored only on company-approved secure servers
  - No local storage on workstations or mobile devices
  - No cloud storage without explicit security team approval
- Transmission Requirements:
  - Must be encrypted during any transmission
  - Must use secure file transfer protocols
  - Must verify recipient authorization before sending
  - Must log all transmissions
- Disposal Requirements:
  - Secure shredding required for physical documents
  - DOD-standard wiping for electronic storage
  - Documentation of destruction required
- Incident Response:
  - Any potential exposure must be reported immediately to Security Team
  - Full incident response plan activation required
  - Regulatory reporting may be required

3.1.2 Confidential Data

- Definition: Business-sensitive information for internal use only
- Examples: Internal financial data, employee records, customer data, business strategies
- Access Requirements:
  - Limited to business need-to-know basis
  - Manager approval required for access

    - Standard authentication required
    - Quarterly access review
- Storage Requirements:
    - Must be stored on company-approved systems
    - Encryption required for mobile device storage
    - Cloud storage allowed only on approved platforms
    - Local storage permitted with encryption
- Transmission Requirements:
    - Encryption required for external transmission
    - Internal transmission via approved company channels only
    - Must verify recipient authorization
- Disposal Requirements:
    - Secure disposal required for physical documents
    - Standard wiping acceptable for electronic storage
    - Documentation recommended but not required
- Incident Response:
    - Report exposure within 24 hours to manager and Security Team
    - Internal investigation required

3.1.3 Internal Use

- Definition: Day-to-day business information not intended for external use
- Examples: Internal communications, procedures, documentation, meeting notes
- Access Requirements:
    - Available to all employees and authorized contractors
    - Standard company authentication required
    - Annual access review
- Storage Requirements:
    - Storage on company systems preferred
    - Local storage permitted
    - Approved cloud storage platforms acceptable
    - Standard company backup procedures apply
- Transmission Requirements:
    - Can be transmitted via standard company email
    - External sharing requires manager approval
    - Must use company-approved sharing methods
- Disposal Requirements:
    - Normal recycling acceptable for physical documents
    - Standard delete acceptable for electronic files
    - No special documentation required
- Incident Response:
    - Report exposure to immediate supervisor
    - Document incident in standard reporting system

3.1.4 Public

- Definition: Information approved for public release
- Examples: Marketing materials, public announcements, published reports
- Access Requirements:

    - No special access controls required
    - Can be shared freely
    - No authentication needed
- Storage Requirements:
    - Can be stored on any system
    - No encryption required
    - Standard backup recommended
- Transmission Requirements:
    - Can be transmitted through any channel
    - No encryption required
    - No special handling needed
- Disposal Requirements:
    - Normal disposal acceptable
    - No special procedures required
- Incident Response:
    - No incident response required for disclosure
    - Document any tampering or unauthorized modifications

4. Password Protection Standards

- **Introduction**: Passwords are the first line of defense against unauthorized access to company systems and information. Strong passwords, when properly managed and protected, significantly reduce the risk of security breaches. This section outlines the company's requirements for creating, using, and protecting passwords to ensure system security while maintaining usability.

4.1 General Password Requirements

4.1.1 Minimum Standards

- At least 8 characters in length
- Contain both upper and lower-case characters
- Include digits and punctuation characters
- Not based on personal information or dictionary words
- Changed every 90 days

4.1.2 Password Protection

- Never write down passwords
- No online storage without encryption
- Do not use Company passwords for non-Company accounts
- Never share passwords with anyone
- Report suspected password compromises immediately

4.2 IT Support Special Requirements (Roles requiring system level access)

- System-level passwords must be changed every 90 days
- Administrative-level passwords must be part of the ITSS password management database
- System-level privileged accounts must use unique passwords
- SNMP strings must be customized from defaults

5. Network Security

- **Introduction**: Network infrastructure is the backbone of business operations and a critical asset requiring robust protection. This section outlines the technical and procedural controls necessary to protect the network from external threats while ensuring reliable access for authorized users. Proper network security is essential for maintaining business operations, protecting sensitive data, and ensuring regulatory compliance.

5.1 Infrastructure Security

5.1.1 Network Segmentation
- Separate networks for different security zones
- VLAN segregation for sensitive systems
- Firewall protection between segments
- Regular network access reviews

5.1.2 Remote Access
- VPN required for remote connections
- Multi-factor authentication mandatory
- Session timeouts enforced
- Regular connection monitoring

5.1.3 Wireless Security
- WPA3 encryption minimum standard
- Separate networks for guests
- Regular security key rotation
- Wireless IPS/IDS monitoring

5.2 Monitoring and Controls

5.2.1 Security Tools
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Security Information and Event Management (SIEM)
- Network Access Control (NAC)
- Regular vulnerability scanning

5.2.2 Patch Management
- Regular security updates
- Critical patches within 24 hours
- Monthly patch compliance review
- Test environment for patches

6. Email and Internet Security

- **Introduction**: Email and internet access are essential business tools that also represent significant security risks if not properly managed. This section provides guidelines for safe and appropriate use of these resources, balancing productivity needs with security requirements. Understanding and following these guidelines helps protect both individual users and the company from various cyber threats including phishing, malware, and data leaks.

6.1 Usage Guidelines

6.1.1 Email Usage

- Business use primary, limited personal use permitted
- No unauthorized advertising or political campaigns
- No inappropriate or unethical content
- Size restrictions on attachments apply
- Encryption required for confidential information

6.1.2 Security Measures

- Report suspicious emails to isitspam@mhgi.net
- Use "Report Message" button for phishing attempts
    - More information on Spam and phishing here:
        - Inspire - News
- Maintain updated virus and malware scanning
- Central storage of mailbox content required

6.1.3 Monitoring

- Company reserves right to monitor all internet traffic
- No expectation of privacy on company systems
- All sites and downloads may be monitored/blocked

7. Device Management

- **Introduction**: Modern business operations rely heavily on various devices, from workstations to mobile phones. Each device represents both an opportunity for productivity and a potential security risk. This section outlines how we manage and secure devices to protect company data while enabling efficient work practices, whether using company-provided or personal devices (BYOD).

7.1 General Device Policies

7.1.1 Company Rights

- Control and manage all corporate data
- Backup, retrieve, modify, or delete data without notice
- Seize and examine devices containing corporate data
- Monitor all device usage

7.1.2 Device Security

- Only approved devices may access company resources
- Updated antivirus software required
- Regular data backups mandatory
- Disk encryption required
- Physical security measures required

7.2 BYOD Requirements

7.2.1 Personal Device Management

- Must separate personal and business data
- Connect through approved VPN when using non-company networks
- Follow all security protocols as company-owned devices
- Report loss/theft immediately

8. Physical Security

- **Introduction**: Physical security is a crucial component of our overall security strategy. Even the strongest cyber security measures can be compromised if physical access to systems and data isn't properly controlled. This section details the company's approach to protecting its facilities, equipment, and information assets from physical threats and unauthorized access.

8.1 Access Controls

8.1.1 Facility Zones

- Zone 1: Entrance and reception
- Zone 2: Support departments
- Zone 3: IT server room
- Zone 4: Business secure areas and workstations

8.1.2 Entry Requirements

- Company access badges required
- Visitor supervision mandatory
- Log entry/exit times
- Video monitoring in restricted areas

8.2 Equipment and Environment

8.2.1 Server Room Requirements

- Temperature maintained between 18-24°C
- No food, drink, or smoking
- Regular maintenance documentation
- Fire suppression systems

8.2.2 Access Management

- Immediate notification of personnel changes
- Return of all access items upon termination
- Regular access review and updates

9. Incident Response

- **Introduction**: Security incidents are inevitable in today's digital environment. The ability to quickly detect, respond to, and recover from security incidents is crucial for maintaining business operations and protecting company assets. This section outlines the company's structured approach to handling security incidents, ensuring consistent and effective response across the organization.

9.1 Response Procedures

- See document 06.005.02 - Cyber Security - Incident Response Plan.docx for detailed procedures to follow in the event of a Cyber Security incident.

9.1.1 Identification

9.1.1 Incident Classification and SLA Tiers

Priority 0 – Business Operations Outage of > 25% or cyber security breach (data breach, ransomware)

- Immediate phone escalation to Director of IT even off hours (24x7x365)
- Director of IT will immediate establishment of war room team and start executing the Incident Response Plan.

Priority 1 - Critical Business Impact (4 hours - 1 Business Day)

- Definition: Restaurant unable to do business through critical sales channel
- Channels affected: drive-through, front counter, kiosk or mobile
- Response: Immediate resolution or work-around required
- Note: Work-around may reduce to Priority 2 for continued investigation

Priority 2 - Speed of Service Impact (3-5 Business Days)

- Definition: Speed of service impact or limited payment ability
- Characteristics: Partial system failure affecting efficiency
- Impact: Reduces restaurant efficiency but channels still functional

Priority 3 - Accuracy and/or Risk Impact (5-10 Business Days)

- Definition: Order accuracy and/or risk impact
- Scope: Systems providing customer feedback, security issues
- Impact: Business risk due to lack of redundancy or compliance

Priority 4 - Customer Experience Impact (10-15 Business Days)

- Definition: Non-food sales, lobby experience, or back of house impact
- Scope: Customer lobby experience or back-office systems
- Impact: Transparent to core restaurant operations

Priority 5 - No Service Impact (15-20 Business Days)

- Definition: No sales or customer impact
- Scope: IT processes only

- Impact: Very low or no impact on restaurant operations

9.1.2 Containment
- Immediate response actions
- System isolation procedures
- Evidence preservation
- Communication protocols

9.1.3 Recovery
- System restoration procedures
- Data recovery processes
- Business continuity activation
- Post-incident analysis

9.1.4 SLA Operating Parameters
- SLA times are maximum goals, team strives to exceed them
- Lower number in range is ideal goal
- Tickets worked as soon as staff available
- Business day calculations apply
- Weekend/holiday support may be limited due to vendor availability
- Time includes vendor ordering and on-site visit scheduling

9.1.5 Escalation Guidelines
- Do not escalate if incident is within SLA
- Use documented escalation process for exceeded SLAs
- Escalation requests for SLA adjustments should be discussed with operations team
- Maintain documented evidence of SLA tracking
- Regular review of SLA effectiveness

- Incident classification criteria
- Initial assessment procedures
- Severity level definitions
- Notification requirements
    - Contact Cybersecurity Insurance provider by issuing an Incident

9.2 Incident Types and Responses

9.2.1 Data Breach
- Customer notification procedures
- Regulatory reporting requirements
- Legal team engagement
    - Contact CFC Cyber insurance provider:
        - CFC Cyber Insurance- How to notify a cyber incident_response app_USA.pdf
- PR response coordination

9.2.2 Malware/Ransomware

- System isolation procedures
- Backup restoration process
- Investigation requirements
- Prevention analysis

10. Business Continuity and Disaster Recovery

- **Introduction**: Ensuring business continuity and having robust disaster recovery capabilities are essential for maintaining critical operations during and after disruptive events. This section outlines company strategies and procedures for maintaining business operations during adverse conditions and recovering quickly from any disruptions.

10.1 Business Continuity

10.1.1 Critical Systems

- System priority levels
- Recovery time objectives
- Recovery point objectives
- Alternative processing procedures

10.1.2 Communication Plans

- Emergency contact procedures
- Stakeholder notification
- External communication protocols
- Status update requirements

10.2 Disaster Recovery

- 10.2.1 Recovery Sites
  - Alternate processing location
  - Data replication requirements
  - Network connectivity
  - Access procedures

- 10.2.2 Recovery Procedures
  - System restoration priority
  - Data synchronization
  - Testing requirements
  - Documentation updates

11. Data Encryption and PCI DSS Compliance

- **Introduction**: Encryption is a critical tool for protecting sensitive data, while PCI DSS compliance is essential for handling payment card information. This section outlines company requirements and procedures for encrypting sensitive data and maintaining compliance with payment card industry standards.

- **11.1 Encryption Requirements**

- 11.1.1 Data Transmission
  - Encryption required for confidential data
  - Secure protocols (VPN, SSH, SSL/TLS) mandatory
  - No plain FTP allowed
  - Digital signatures for sensitive external communications

- 11.1.2 Payment Data Security
  - PCI-DSS compliance mandatory
  - PA-DSS certified systems required
  - No storage of CVV codes, track data, or PINs
  - Third-party PCI certification required

- **11.2 Key Management**
  - Authorized user access to encrypted data
  - Compliance with retention requirements
  - Regular key rotation and management
  - Documentation of all key changes

12. Training and Accountability

- **Introduction**: Security awareness and training are essential components of the company's security program. Even the best security policies and technologies can be compromised without proper user awareness and adherence. This section outlines the approach to ensuring all employees understand and follow security requirements.

- **12.1 Training Requirements**
  - Regular security awareness training
  - Social media privacy awareness
  - Phishing and social engineering awareness
  - Procedure and policy updates

- **12.2 Compliance**
  - Regular monitoring of policy compliance
  - Violations may result in disciplinary action
  - Immediate reporting of security incidents
  - Regular policy review and updates

13. Review and Updates

- Information and Cyber Security Policy changes will be assessed at least annually or upon a change with impact to said policies.

13.1 Review Process

13.1.1 Annual Review

- Policy effectiveness assessment
- Threat landscape review
- Compliance requirement updates
- Stakeholder feedback
- Executive leadership team review

13.1.2 Update Procedures

- Change documentation
- Approval requirements
- Communication plan
- Training updates

meritage HOSPITALITY GROUP

Response Plan

Effective Date: 2025

Policy Number: 06.005.03

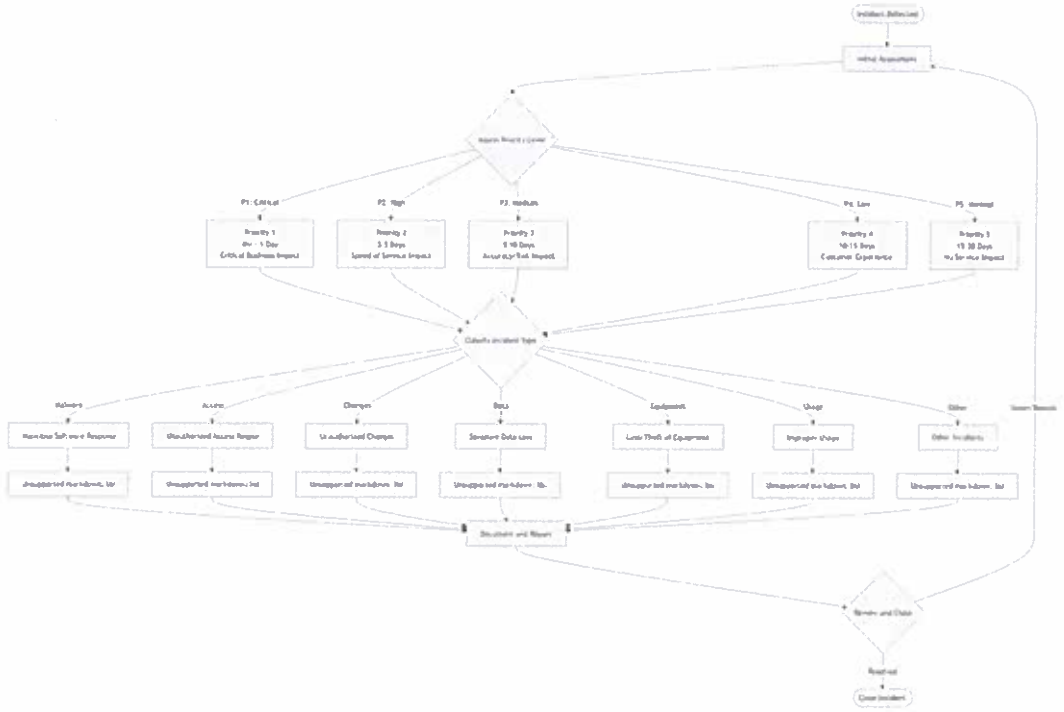
Business Continuity & Cyber Security Incident Response Plan

1. Plan Overview

Computer incident response has become an important component of information security (IT) programs. The threat landscape of computer systems is constantly changing, and every organization must be prepared for any threat they may encounter. This plan outlines the process of handling any computer incident while focusing on the more commonly encountered attack categories.

2. Scope

The Incident Response Policy applies to all employees, executives, contractors, and vendors with access to any part of the information technology network of this enterprise, regardless of role. Any intrusion, no matter how it's discovered, must be reported under the procedures outlined by this policy.



3. Incident Response Team Contacts

When a security incident occurs contact the following individuals. Start at the top of the list and move down until you reach someone. The person contacted will determine who to escalate the issue to.

Primary Contacts (24/7):

- System Administrator – [redacted]
- System Administrator – [redacted]
- System Administrator – [redacted]
- Director of IT – [redacted]

After Hours Escalation:

- On-call Security Team: [redacted]
- IT Emergency Response: [redacted]

4. Incident Definition and Classification

An incident requiring action is defined as an adverse event that has caused, or has the potential to cause, damage to the assets, reputation, or personnel of the enterprise.

4.1 Severity Levels and Response Times

Priority 0 – Business Operations Outage of > 25% or cyber security breach (data breach, ransomware)

- Immediate phone escalation to Director of IT even off hours (24x7x365)
- Director of IT will immediate establishment of war room team and start executing the Incident Response Plan.

Priority 1 - Critical Business Impact (4 hours - 1 Business Day)

- Definition: Restaurant unable to do business through critical sales channel
- Channels affected: drive-through, front counter, kiosk or mobile
- Response: Immediate resolution or work-around required
- Note: Work-around may reduce to Priority 2 for continued investigation

Priority 2 - Speed of Service Impact (3-5 Business Days)

- Definition: Speed of service impact or limited payment ability
- Characteristics: Partial system failure affecting efficiency
- Impact: Reduces restaurant efficiency but channels still functional

Priority 3 - Accuracy and/or Risk Impact (5-10 Business Days)

- Definition: Order accuracy and/or risk impact
- Scope: Systems providing customer feedback, security issues
- Impact: Business risk due to lack of redundancy or compliance

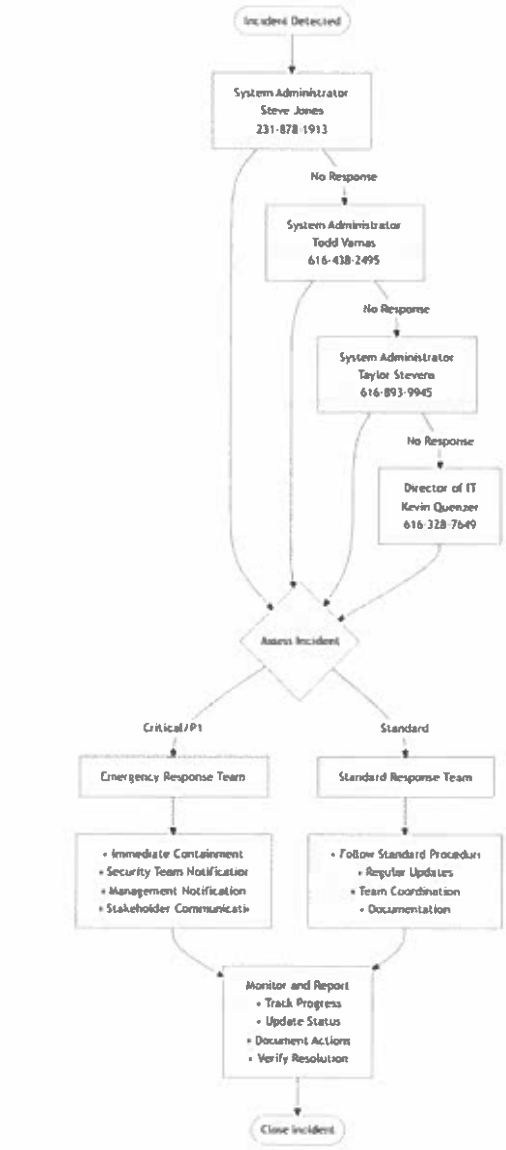
Priority 4 - Customer Experience Impact (10-15 Business Days)

- Definition: Non-food sales, lobby experience, or back of house impact
- Scope: Customer lobby experience or back-office systems
- Impact: Transparent to core restaurant operations

Priority 5 - No Service Impact (15-20 Business Days)

- Definition: No sales or customer impact
- Scope: IT processes only
- Impact: Very low or no impact on restaurant operations

5. Initial Response Procedures



5.1 Immediate Actions

0. If Incident Severity is P0 (highest) the Director of IT will immediately establish a business continuity war room.

1. Document initial discovery:

- Date and time of discovery
- How the incident was discovered

- Systems/data potentially affected
- Current impact on business operations

2. Preserve evidence:

- Create system backup if possible
- Screenshot error messages/logs
- Document unusual system behavior
- Preserve security camera footage if relevant
- Maintain chain of custody documentation

3. Containment:

- Isolate affected systems
- Disable compromised accounts
- Block suspicious IP addresses
- Preserve system logs
- Document all actions taken

5.2 Incident Reporting Form Requirements

All incidents must be documented using the standard Incident Report Form including:

- Incident identifier
- Classification and severity
- Systems/data affected
- Timeline of events
- Actions taken
- Evidence collected
- Personnel involved
- Business impact assessment

6. Attack Categories and Response Procedures

6.1 Malicious Software Infection

The following response actions may be performed by any company IT staff with sufficient training, knowledge, and access to perform the actions.

Required Steps:

1. Immediately notify the Meritage IT Security Specialist.
2. Identify the infected system(s).
3. Isolate the system(s):
   - Disconnect from all networks if possible
   - For remote machines without physical access:
     - Connect to an isolated network (such as guest wifi)
     - Access through GoToAssist
   - If machine is not functional enough for remote access:
     - Ship to corporate office for further analysis
4. Run Symantec Endpoint Protection:
   - Perform full system scan
   - If infection detected:
     - Remediate the infection
     - Run scan again
     - Repeat until passing scan achieved
5. Run Malwarebytes:
   - Perform full system scan
   - If infection detected:
     - Remediate the infection
     - Run scan again
     - Repeat until passing scan achieved
6. Post-Resolution:
   - Attempt to identify cause of infection

- Coach employee if appropriate
- Document all actions taken and findings

6.2 Unauthorized Access

1. Immediate Actions:
   - Notify IT Security Specialist
   - Lock affected accounts
   - Enable enhanced logging
   - Document suspicious activity

2. Investigation:
   - Review access logs
   - Identify compromised systems
   - Document unauthorized changes
   - Preserve evidence

3. Recovery:
   - Reset compromised credentials
   - Revert unauthorized changes
   - Implement additional controls
   - Verify system integrity

4. Post-Incident:
   - Update access controls
   - Enhance monitoring
   - Review security policies
   - Document lessons learned

6.3 Data Loss/Theft

1. Immediate Actions:
   - Notify IT Security Specialist
   - Identify lost/stolen data
   - Document scope of loss
   - Begin chain of custody log

2. Investigation:
   - Review access logs
   - Identify data exposure
   - Document unauthorized access
   - Assess regulatory impact

3. Notification Requirements:
   - Identify affected parties
   - Prepare notification messages
   - Follow regulatory requirements
   - Document all communications

4. Recovery:
   - Secure remaining data
   - Implement new controls
   - Update security policies
   - Enhance monitoring

6.4 Equipment Loss/Theft

1. Immediate Actions:
   - Notify IT Security Specialist

- Report to law enforcement
- Document lost assets
- Enable remote wipe if available

2. Response:
   - Disable device access
   - Change related credentials
   - Document potential data exposure
   - Notify affected parties

3. Recovery:
   - Replace equipment
   - Restore from backup
   - Update asset inventory
   - Enhance physical security

7. Communication Protocols

7.1 Internal Communication

- Use secure communication channels
- Follow defined escalation paths
- Document all communications
- Maintain confidentiality

7.2 External Communication

- Director of IT will immediately communicate to Executive Leadership for P0 incidents and determination on external response.
- PR/Media Response Template:
  - Acknowledge incident
  - Describe impact

- Detail response actions
- Provide next steps

- Customer Notification Requirements:
  - Timing requirements
  - Content requirements
  - Delivery methods
  - Follow-up procedures

8. Post-Incident Procedures

8.1 Analysis Requirements

1. Incident Summary Report:
   - Timeline of events
   - Impact assessment
   - Response effectiveness
   - Recommendations

2. Lessons Learned:
   - What worked well
   - What needs improvement
   - Policy/procedure updates
   - Training needs

8.2 Documentation Requirements

1. Final Report Contents:
   - Executive summary
   - Technical details

- Business impact
- Corrective actions
- Prevention measures

2. Record Retention:
   - Maintain all documentation for 3 years
   - Secure storage of sensitive data
   - Chain of custody records
   - Communication logs

9. Training and Updates

- Annual incident response training
- Quarterly tabletop exercises
- Regular plan updates
- Lessons learned integration

10. Policy Review

This policy will be reviewed and updated annually or upon significant changes to the business or threat landscape.

Last Updated: December 2024

Next Review: January 2026