SECURITY POLICY

1 Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contractors as applicable.

2 Information Security Policy

BGB handles sensitive cardholder information daily. Sensitive information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation. BGB commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises. Employees handling sensitive cardholder data should ensure:

- Handle BGB and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of the BGB information and telecommunication systems and ensure it doesn't interfere with your job performance;
- BGB reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other BGB resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personal information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your direct manager.

3 Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the BGB established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. BGB will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes cardholder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from BGB email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the BGB, unless posting is in the course of business duties and separately approved by the management.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses or Trojan horse code.

4 Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

5 Protect Stored Data

All sensitive cardholder data stored and handled by BGB and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by BGB for business reasons must be discarded in a secure and irrecoverable manner.

- If there is no specific need to see the full PAN (Primary Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, messenger and etc.
- It is strictly prohibited to store:
- The content of the payment card details on any media whatsoever.
- The content of the transaction, including all transaction details on any media whatsoever.
- The PAN or the encrypted PAN Block under any circumstance.

6 Information Classification

Data and media containing data must always be labelled to indicate sensitivity level:

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to BGB if disclosed or modified. Confidential data includes cardholder data.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure.
- **Public data** is information that may be freely disseminated.

7 Access to Sensitive Cardholder Data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

1. Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
2. Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities.
3. Privileges should be assigned to individuals based on job classification and function (Role based access control).
4. Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
5. No other employees should have access to this confidential data unless they have a genuine business need.
6. If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
7. BGB will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
8. BGB will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
9. BGB will have a process in place to monitor the PCI DSS compliance status of the Service provider.

8 Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes cardholder data.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.

- Media is defined as any printed or handwritten paper, received faxes, disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on BGB sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- Strict control is maintained over the external or internal distribution of any media containing cardholder data and has to be approved by management.
- Strict control is maintained over the storage and accessibility of media.
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9 Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Cardholder data (PAN, track data etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC, etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10 Disposal of Stored Data

- All data must be securely disposed of when no longer required by BGB, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- BGB will have procedures for the destruction of hard-copy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- BGB will have documented procedures for the destruction of electronic media. These will require:

    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” – access to these containers must be restricted.

11 Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Company.
- All third parties with access to credit card account numbers are contractually obligated to comply with required level of card association security standards (PCI DSS).
- Company security policies must be reviewed annually and updated as needed.

12 Network Security

- Firewalls or VPN must be implemented at each internet connection and any demilitarized zone (DMZ) and the internal company network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the cardholder data environment.
- Firewall technology must be implemented where the Internet enters the Company network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall or using VPN access.

13 System and Password Policy

All users, including contractors and vendors with access to BGB systems, are responsible for taking the appropriate steps, as outlined in BGB Password Policy.

14 Anti-Virus Policy

- All machines must be configured to run the latest anti-virus software as approved by BGB. The preferred application to use is Symantec Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all required systems.
- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to modify and any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any email, which they suspect may contain virus.

15 Patch Management Policy

- All Workstations, servers, software, system components etc. owned by BGB must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Wherever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within two months of release from the respective vendor and have to follow the process in accordance with change control process.
- Any exceptions to this process have to be documented.

16 Remote Access Policy

- It is the responsibility of BGB employees, contractors, vendors and agents with remote access privileges to BGB's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to BGB.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentications via one-time password authentication or public/private keys with strong passphrases.
- Vendor accounts with access to the company network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to BGB internal networks via remote access technologies will be monitored on a regular basis.

- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.

Vendor accounts with access to BGB network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

17 Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as Common Vulnerability Scoring System (CVSS) base score.
- As part of the PCI-DSS Compliance requirements, BGB will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by BGB internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the BGB's internal staff. The scan process should include re-scans until passing results are obtained.

18 Configuration Standards

- Information systems that process transmit, or store cardholder data must be configured in accordance with the applicable standard for that class of device or system. Standards must be written and maintained by the team responsible for the management of the system in conjunction with the Information Security responsible employees.
- All network device configurations must adhere to BGB required standards before being placed on the network as specified in BGB configuration guide. Using this guide, a gold-image configuration has been created that will be applied to all network devices before being placed on the network.
- Before being deployed into production, a system must be certified to meet the applicable configuration standard.
- Updates to network device operating system and/or configuration settings that fall under BGB standards are announced by the Information security responsible employees.
- Updates must be applied within the time frame identified by the Information security employees.
- Administrators of network devices that do not adhere to BGB standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.
- All network device configurations must be checked annually against the configuration gold-image to ensure the configuration continues to meet required standards.

- Where possible, network configuration management software will be used to automate the process of confirming adherence to the gold-image configuration.
- For other devices, an audit will be performed quarterly to compare the gold-image configuration to the configuration currently in place.
- All discrepancies will be evaluated and remediated by Network Administration.

19 Change Control Process

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.
- All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, maintained at a Business level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependant on the outcome, impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.
- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.
- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.
- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention policies.
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.
- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.
- Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result

(as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for assessment.

20 Audit and Log Review

- Separate procedure will be conducted which will covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over BGB network, including the following components and main principles listed below:
    - Operating System Logs (Event Logs).
    - Firewalls & Network Logs.
    - Antivirus Logs.
- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
- The BGB IT personnel are the only people permitted to access log files.

21 Secure Application Development

- The Secure Application development policy is a plan of action to guide developers' decisions and actions during the software development lifecycle (SDLC) to ensure software security. This policy aims to be language and platform independent so that it is applicable across all software development projects.
- The adherence to and use of Secure Application Development Coding Policy is a requirement for all software development on BGB information technology systems and trusted contractor sites processing BGB data.
- Each phase of the SDLC is mapped with security activities, as explained below:

1. a) Design

- Identify Design Requirements from security perspective
- Architecture & Design Reviews Threat Modelling

1. b) Coding

- Coding Best Practices
- Perform Static Analysis

1. c) Testing

- Vulnerability Assessment
- Fuzzing

1. d) Deployment

- Server Configuration Review
- Network Configuration Review
- Development of code shall be checked and validated with the most current versions of BGB Coding Standards for Secure Application Development. All code developers shall verify that their code is in compliance with the most recent and approved coding standards and guidelines.
- Only validated code shall be implemented into BGB production environment. A review and validation ensures that code exhibits fundamental security properties to include correctness, predictability, and attack tolerance.

Application Code Developers shall:

- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.
- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended.
- Coding techniques must address injection flaws particularly SQL injection, buffer overflow vulnerabilities, cross site scripting vulnerabilities, improper access control (insecure direct object reference, failure to restrict URL access, directory traversal etc.,), cross site request forgery (CSRF), broken authentication and session management.
- Never trust incoming data to the system, apply checks to this data.
- Never rely on the client to store sensitive data no matter how trivial.
- Disable Error messages that return any information to the user.
- Use object inheritance, encapsulation, and polymorphism wherever possible.
- Use environment variables prudently and always check boundaries and buffers.
- Applications must validate input to ensure it is well-formed and meaningful.

22 Penetration Testing Methodology

Tests must follow the OSSTMM methodology. Tests must be conducted at network, system and application level and must ensure that at least identifies any vulnerabilities documented by OWASP and SANS, as well as those identified in the PCI DSS standard v3.

Tests preferably should be performed by the external suppliers with full support of BGB IT department, that need to cover following subjects:

- External intrusion tests will be performed remotely from the supplier's premises. Internal intrusion tests will be conducted in the office BGB of the Organization. Audit team must to have access to the Organization's network. It must manage access permissions to the building early enough to ensure that the audit team can access without problems during planning period.
- All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.
- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organization, the incident should be brought

immediately to the attention of those responsible for incident management in the project.
- It should be noted that in order to comply with PCI DSS the scope of the test should include, at least the following:
    - All systems and applications that are part of the perimeter of the cardholder data environment card (CDE).

For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.

As a result of tests performed should generate a document containing at least the following sections:

- Introduction
- Executive Summary
- Methodology
- Identified vulnerabilities
- Recommendations for correcting vulnerabilities
- Conclusions
- Evidence

23 Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to BGB communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

The Incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Employees of the company will be expected to report to the security officer for any security related issues.

The Company PCI security incident response plan is as follows:

1. BGB employees must report an incident to the Information Security responsible employees or to another member of the IT Team.
2. Information Security Team will investigate the incident and assist the potentially compromised employee in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
3. Information Security Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
4. Information Security Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
5. If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Security

officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.

6. Employee or employees that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform BGB Information Security Team. After being notified of a compromise, the Information Security Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment employees' response plans.

BGB Information Security Team:

- CIO;
- Head of Underwriting and Risk;
- Head of Legal;
- Head of Finance;

Incident Response Notification:

Escalation

- BGB Members of the Board

External Contacts (as needed)

- Merchant Provider
- Card Brands
- Internet Service Provider (if applicable)
- Internet Service Provider of Intruder (if applicable)
- Business Partners
- Insurance Carrier
- External Response Team as applicable (CERT Coordination Centre 1, etc.) Law

In response to a systems compromise, BGB Information Security Team and designees will:

- Ensure compromised system/s is isolated on/from the network.
- Gather, review and analyse the logs and related information from various central and local safeguards and security controls
- Conduct appropriate forensic analysis of compromised system.
- Contact internal and external departments and entities as appropriate.
- Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
- Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The card companies have individually specific requirements, the BGB Information Security Team must address in reporting suspected or confirmed breaches of cardholder data.

Incident Response notifications to various card schemes:

- In the event of a suspected security breach, alert the information security officer or your direct manager immediately.

- The security officer will carry out an initial investigation of the suspected security breach.
- Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

23.2 Visa Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.

23.3 Mastercard Steps

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

Employees of BGB will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions,

monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implementation of the incident response plan in the event of a sensitive data compromise.

23.4 Discover Steps

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention;
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances;
3. Prepare a list of all known compromised account numbers;
4. Obtain additional specific requirements from Discover Card.

23.5 American Express Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express.

24 Roles and Responsibilities

Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include:
    - Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
- The Information Technology department (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).
- System and Application Administrators shall:
    - monitor and analyse security alerts and information and distribute to appropriate personnel administer user accounts and manage authentication
    - Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.
- The Human Resources department (or equivalent) is responsible for tracking employee participation in the security awareness program, including:
    - Facilitating participation upon hire and at least annually.

    - Ensuring that employees acknowledge in writing at least annually that they have read and understand the Company's information security policy.
- Legal department (or equivalent) will ensure that for service providers with whom cardholder information is shared:
    - Written contracts require adherence to PCI-DSS by the service provider.
    - Written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.

25 Third Party Access to Cardholder Data

- All third-party companies providing critical services to BGB must provide an agreed Service Level Agreement (SLA).
- All third-party companies providing hosting facilities must comply with BGB's Physical Security and Access Control Policy.
- All third-party companies which have access to Cardholder information must:
    - Adhere to the PCI DSS security requirements.
    - Acknowledge their responsibility for securing the Cardholder data.
    - Acknowledge that the Cardholder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
    - Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
    - Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

26 User Access Management

- Access to BGB is controlled through a formal user registration process beginning with a formal notification from HR or from a direct manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/direct management.
- The job function of the user decides the level of access the employee has to cardholder data.
- A request for service must be made in writing (email or hard copy) by the newcomer's direct manager or by HR. The request is free format, but must state:
    - Name of person making request:
    - Job title of the newcomers and workgroup:
    - Start date:
    - Services required:
- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all BGB systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves BGB employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or direct managers in the case of contractors) will inform IT department of all leavers and their date of leaving.

27 Access Control Policy

- Access Control systems are in place to protect the interests of all users of BGB computer systems by providing a safe, secure and readily accessible environment in which to work.
- BGB will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT department. IT team shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of noncompliance to the BGB CIO.
- Access to BGB IT resources and services will be given through the provision of a unique account and complex password.
- No access to any BGB IT resources and services will be provided without prior authentication and authorization of a user's BGB Active Directory or LDAP account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Active Directory or LDAP Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by BGB policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the guidance of Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access control methods include logon access rights, share drives and access permissions, user account privileges, server and workstation access rights, firewall and VPN permissions, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

28 Wireless Policy

If the need arises to use wireless technology, it should be approved by the company and the following wireless standards have to be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the company.
2. The firmware on the wireless devices has to be updated accordingly as per vendor's release schedule.
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data or via RADIUS protocol.
6. An Inventory of authorized access points along with a business justification must be maintained. (Update Appendix B).

APPENDIX A – AGREEMENT TO COMPLY WITH INFORMATION SECURITY POLICY

_____
IS Policy version

_____
Employee Name (printed)

_____
Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the Company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner. I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Company security policy. I understand that noncompliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____
Employee Signature

APPEDNIX B

Assets and Devices:

Asset/ Device Name	Description	Owner/ Approved User	Location

List of Service Providers:

Name of Service Provider	Contact Details	Provided Service	PCI DSS Compliant and level	PCI DSS Validation date	Reference/Details