GREATER BOSTON CONVENTION & VISITORS BUREAU

INTERNAL CONTROL GUIDE

UPDATED JULY 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Greater Boston Convention & Visitors Bureau has developed an Internal Control Plan to assess risks faced by the GBCVB and to assist our senior management in meeting the mission and objectives established by our Board of Directors. Our plan focuses on providing reasonable assurance that the GBCVB 's assets are safeguarded against loss from unauthorized use or disposition. This plan also ensures that all our financial transactions are transparent and executed in accordance with senior management's authorization and are recorded properly to permit the preparation of financial statements in accordance with generally accepted accounting policies (GAAP).

The responsibility of designing and implementing internal controls is a continuous process as conditions change, and therefore, control procedures may become outdated and inadequate. Our business focus, actions and values set the tone for the GBCVB as an organization. Our approach is to establish as a fundamental underpinning of the Bureau that senior management view internal controls as critically important and we communicate that message and tone to all our employees at all levels, to our Board of Directors, and to our member companies.

The GBCVB's Internal Control Plan is an important reference document used by the GBCVB's senior management and all employees. It is designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. Our internal control plan helps senior management be effective and efficient while avoiding serious problems such as overspending, operational failures and violations of laws.

Internal controls must benefit rather than hinder the organization, they are not stand-alone practices, must be woven into the day to day responsibilities of all staff and lastly be cost effective.

July 2018

Patrick B. Moscaritolo
President & CEO

VISION AND MISSION STATEMENTS

(GBCVB) VISION

1. To develop the best one-stop sales and service organization for meeting planners and visitors worldwide;

2. Establish policies, procedures and practices that are in compliance with applicable Laws, Regulations and Industry Standards;

3. Identify, evaluate and implement creative and practical approaches to achieve our mission in the most cost-effective manner;

4. Engage our stakeholders and members as partners in the GBCVB's mission, goals and role in the region;

5. Provide a professional and rewarding environment for staff.

(GBCVB) MISSION

To fulfill our mission of increasing business and revenue for our members and creating jobs and economic growth for our region, the GBCVB will attract conventions, meetings and visitors to Boston, Cambridge and our region through

1. Direct sales and marketing programs in major market centers in the U.S. and across the globe;

2. Developing and promoting special events that generate hotel room nights and business for our members;

3. Providing a full range of visitor publications and services;

4. Carrying out a comprehensive worldwide public relations and promotions program involving local, national, and international media, as well as consumer and trade publications worldwide;

5. Carrying out a comprehensive destination marketing program in collaboration with our members, the Massachusetts Office of Travel & Tourism, Massport, the Massachusetts Convention Center Authority, the City of Boston's Mayor's Office of Arts, Tourism & Special Events and the Cambridge Office for Tourism.

HOW THE GBCVB CONTROLS AGAINST RISKS:

The GBCVB has developed a Risk Assessment Plan which is concerned with identifying and analyzing the risks to the organization and determining what should be done about them. The plan provides guidance and structure and focuses on providing an ongoing, comprehensive and systematic approach to problem solving and reducing risk exposures. Risk management activities include identifying, investigating and evaluating risks followed by selecting and implementing the most appropriate method of correcting, reducing, managing, transferring or eliminating the risks. The GBCVB has analyzed the effectiveness of the internal controls system in the following areas:

- Control Environment
- Risk Assessment
- Control Activities
- Monitoring
- Information and Communications

CONTROL ENVIRONMENT:

The GBCVB has conducted an Organizational Risk Assessment to determine which factors might prevent the GBCVB from attaining its stated mission. The President & CEO as head of the organization manages the budgeting with the assistance of senior management and Department Heads. Budgets are reviewed and approved bi-annually by the Board's Finance Committee and Board of Directors.

The GBCVB's organizational structure, policies, and procedures set the proper foundation for internal controls, providing structure and discipline as well as encompassing both technical and ethical commitment. The GBCVB is committed to hiring and training qualified staff. The majority of the GBCVB's administrative and oversight activities, including outside contracting, accounting and budgeting are managed by the President and senior staff. The President and senior management staff meet regularly to stay current on industry information, and issues that may need to be addressed through policies and procedures. The Department Heads have on going meetings with their staff to review projects, budgets and procedural matters.

Contracts are reviewed in accordance with our vendor policy. The Director of Finance oversees an annual audit which is conducted by a certified public accounting firm and then is reviewed and approved by the GBCVB's Finance Committee and Board of Directors annually. The computer systems maintenance and security are overseen by iCorps under the supervision of the Sr. Vice President of Administration and the Vice President of Operations.

The Board's Finance Committee and Board of Directors each meet quarterly to review the budget, programs and operations of the organization and both have minutes recorded and included in our annual audit reviews. The Board of Directors adheres to guidelines established for their participation on the Board and signs and submits a Conflict of Interest Disclosure and Antitrust Compliance forms annually.

The GBCVB has a policy and procedures manual which is updated on a regular basis by the Human Resources department and senior management with the President's approval.

The GBCVB has established, detailed job descriptions and formal evaluations for its employees. The GBCVB believes it is essential to provide educational and training opportunities for staff to enable them to continuously develop their skills and abilities.

RISK ASSESSMENT:

A Risk Assessment is the process used to identify, analyze, and manage the potential risks that could hinder or prevent the achievement of our goals and objectives. It allows the GBCVB to understand the extent to which potential events may impact objectives. Risks are assessed from both the likelihood of happening and the impact if it happens. The GBCVB on a regular basis meets with an outside CPA, who serves as the Treasurer of the Board and Chair of the GBCVB Finance Committee, provides pro bono professional advice and assistance regarding financial procedures of internal controls. This approach allows us to:

1. Assess how significant the risk's impact might be on the GBCVB
2. Take actions to eliminate or minimize risks
3. Provides ongoing monitoring of the potential risk

The GBCVB believes that an assessment of risks from both internal and external sources is a crucial part of enhancing the overall performance of the organization. To ensure the GBCVB is meeting our mission, we have considered the following questions or standards in developing a risk assessment plan:

Is there adequate connections between the activity objective and the Bureau's mission and goals?

Does a particular activity or program affect another area of the organization?

Does a particular activity or program affect our members and stakeholders outside of the organization?

What are the qualifications of personnel and vendors hired and what methods are used to train staff about their job duties?

Are there responsible and adequate staff resources available to perform an activity that exposes risk to the GBCVB?

In addition to looking at these questions the GBCVB management and staff have considered a wide range of potential issues, as well as the likelihood and frequency of the risks occurring. We have narrowed the list to seven risks and have determined how we want to manage the risks by determining what steps need to be taken to eliminate or reduce the risk to an acceptable level. These risks are identified with action steps in the Risk Analysis Summary Overview Section.

CONTROL ACTIVITIES:

The Greater Boston Convention & Visitors Bureau's control activities include policies, procedures, and directives that occur at all levels and functions. The control activities are established to minimize the identified risks including structure, policies and procedures. The GBCVB's organizational structure, policies and procedures are subject to ongoing review by a number of entities. Because the Board places such a high priority on financial management and internal controls, there are a number of review and evaluation elements built into our operations.

Our financial procedures and guidelines are discussed quarterly at the Board's Finance Committee meetings. As previously stated an outside CPA who serves as the Treasurer of the Board and Chair of the GBCVB Finance Committee provides pro bono professional advice and assistance regarding our financial matters, procedures and internal controls and provides us a list of recommended guidelines they have implemented for their other non-profit clients.

In addition, an annual Bureau wide audit is conducted by PKF, a national CPA firm, who administers testing, and review our internal controls in the financial as well as the personnel areas and make recommendations that they present to our Board's Finance Committee.

The GBCVB's internal control policies and procedures are based on management's assessment of the risks involved for each activity. We have developed policies and procedures and other documents to control risk in order to ensure that the GBCVB meets its goals and objectives, efficiently and effectively using available resources. The GBCVB also has adopted a written information security program (WISP) in an effort to better safeguard Personnel information that it may collect, store or maintain in its records.

INTERNAL CONTROL KEY CONCEPTS:

I. **Separation of Duties**:

A primary principle of an internal control plan is the separation of duties that help protect against misuse of funds. In the automated environment, the principle of separation is critical because it ensures the segregation of different functions, such as data preparation, input and review. It also defines responsibility over transactions and use of resources.

The following activities are properly separated at the GBCVB:

1. Payroll Activities

    a. Payroll is processed on a biweekly basis by the Financial Management Analyst. Any payroll changes (new hires, terminations, rate changes etc.) are originated by Human Resources or Department heads. All payroll changes are approved by President and Senior Vice President of Administration and the payroll preview is reviewed and approved by the President or the Senior Vice President of Administration before final processing. When payroll package is received the following day, the President or the Senior Vice President reviews and approves final payroll report to prevent any interim changes being made.

2. Accounts Payable

    a. All approved invoices are entered into the accounting system on a daily basis by the Financial Management Analyst. On a weekly basis, selected invoices to be paid by due date and/or priority are determined. When invoices are posted, the Financial Management Analyst prints weekly edit report from Great Plains which is reviewed and approved (along with the invoices to be paid) by Director of Finance prior to the checks being printed.

    b. Checks are printed from blank check stock. Once the check run is completed, invoices are reviewed, and checks are signed by the President or Senior Vice President of Administration. The check run is then given to the Accounts Receivable Coordinator to mail or distribute.

3. Accounts Receivable

    a. Checks that are mailed directly to the GBCVB are given to the Financial Management Analyst who then creates a simple spreadsheet identifying the

Payer, check number, check date and amount. The checks are recorded in an Aging Report.

b. The checks are then locked in the Director of Finance's office. The Accounts Receivable Coordinator retrieves the checks from the locked cabinet, prepares the electronic deposit and compares the deposit ticket and tape total.

c. Completed deposits are given to the Director of Finance for review and approval. Director of Finance compares the Financial Management spreadsheet against the deposit tape and then approves the deposit amount.

d. Director of Finance checks the bank account on line the next day to ensure that the approved deposit amount was posted to the bank account.

e. After the electronic deposit is made, the Accounts Receivable Coordinator enters the cash receipts into the accounting system (Great Plains) and prepares the edit sheet for the Director of Finance for approval prior to posting. Invoices created by the Accounts Receivable Coordinator go through this same approval process.

f. Accounts Payable and Accounts Receivable entries are posted throughout the month. When the A/P and A/R modules are closed for the month, the Director of Finance prints trial balances which are compared and reconciled with the general ledger. Financial Management Analyst and Accounts Receivable Coordinator maintain manual logs which are approved by the Director of Finance to ensure that month end totals tie correctly.

g. Accounts Receivable statements are printed by the Accounts Receivable Coordinator on a monthly basis and submitted to the Director of Finance for review before mailing. All credit memos are reviewed and approved by the Director of Finance. Collection is done via email or by telephone. Financial Management Analyst follows up frequently on delinquent amounts and if payment is not received within a reasonable amount of time, appropriate action is taken. Accounts Receivable Aging Reports are reviewed monthly by Director of Finance.

4. Bank Reconciliations

a. All cash accounts are reconciled monthly.

b. Director of Finance reconciles the operating account because Financial Management Analyst handles all disbursements from the operating account

and Accounts Receivable Coordinator handles the bank deposits.

c. Online cash transfers are originated by the Financial Management Analyst, approved by the Director of Finance and the President or the Senior Vice President of Administration. The Director of Finance then releases the wires on-line through electronic banking.

d. Monthly reconciliations and bank statements are reviewed by Director of Finance.

5. Petty Cash/Check Requests/Credit Cards

a. Petty cash is available from the Financial Management Analyst for small cash purchases. Petty cash requests are limited to a maximum of $100.00 per request. If an employee requires a larger amount, they must request it via a check request form. Forms must be completed with date of request, employee name, description, account and department code, amount and appropriate director's approval. If employee pays for the item with their own funds, the receipt must be attached to the petty cash/check request form before reimbursement can be made.

b. Check Request Forms are used for all payments made by the GBCVB that are not submitted by a vendor's invoice. Checks are normally written every Thursday and require a minimum of one week to process. Forms must be completed with date requested, date required, and payee of check, description, general ledger account and with appropriate Director or V/P approval. Check requests are used for all payments made by the GBCVB that are not submitted by a vendor's invoice. A check request over $25,000 must be approved in advance by the President & CEO and the Sr. Vice President.

c. A check or credit card request over $25,000 must be approved in advance by the President & CEO and the Sr. Vice President. The President or Sr. Vice President of Administration reviews and signs the check runs weekly.

d. Certain employees are issued a company American Express credit card with the annual fee paid by the GBCVB. The employee is responsible for paying the charges each month by the payment deadline and therefore must submit their expense report promptly so that they are reimbursed in time to pay the monthly charges. Failure to do this will result in discontinuation of the credit card. Any credit card charges over $25,000 will not be approved without two signatures (President and the Sr. Vice President).

6. Expense Reports

    a. The GBCVB will reimburse employees for reasonable and proper expenses incurred in the conduct of the Bureau's business.

    b. Generally, the employee traveling should provide a written estimate of the anticipated costs (e.g., airfare, hotel accommodations, meals, registration fees, etc.) for advance approval by the Department Director/Vice President/ Sr. Vice Presidents and/or the President. (All travel expenses must be within departmental limits established in the GBCVB's annual budget.)

    c. Prudent judgment must be exercised when incurring travel and/or business expenses. Good business practice requires that all expenditures be clearly and correctly recorded; that any unusual amount be fully explained in writing. Receipts must be provided for lodging and all other expenses for which receipts are normally obtainable. If receipts are lost or otherwise not available, a written explanation of their unavailability must accompany the expense report. Such a written explanation shall in addition to explaining why a receipt is unavailable, specify the date of the expenditure and where incurred (place of purchase). Under federal law, expenses without a receipt may be reimbursed up to $25.

    d. Department Directors/Vice Presidents/Sr. Vice Presidents and/or the President are responsible for reviewing all travel/business expenses to be charged to their budget, and for verifying that such expenses are reasonable and proper and in accordance with the GBCVB Travel and Business Expense Policy and Procedure and within budget. Their signature on the Expense Report indicates that such responsibility has been satisfied and is required before the report will be accepted for processing by the Finance Department. The expense reports for the President and CEO are reviewed and approved by the Senior Vice President and the Director of Finance.

7. Journal Entries/Financial Statements

    a. Director of Finance prepares monthly journal entries as well as any adjustments, prepares edit reports from Great Plains (similar to the other accounting processes mentioned above) and reviews and approves prior to posting. Complete financial statements are distributed on a monthly basis to the President and Senior Vice President of Administration including a balance sheet and general ledger detail. Other senior management receive financial statements and general ledger details for their respective departments. Financial Statements are audited on an annual basis by an

outside CPA firm. A separate audit is performed annually by the same CPA firm for the 1038 Grant.

b. Because of the limited number of personnel, close and documented review and approval of transactions, reports and reconciliations is especially critical.

8. Purchase of Services/Purchase Orders

a. Purchase Orders (P.O.) are required for all goods and services purchased except for UPS and U.S. mail. Employees do not have the authority to commit the GBCVB to any expenditure without obtaining a properly approved Purchase Order. Requests for purchases should be submitted on Purchase Order and approved through appropriate policy. The P.O. must be approved by Department Director with budget code and then approved by the Director of Finance. Any requests over $25,000 will not be approved without two signatures (President and the Sr. Vice President).

b. Funds must be available before the purchase and no purchase can be made without proper approved authorization in advance.

c. When an invoice is received, it will be matched to the Purchase Order for processing into the accounting system. If the invoice and Purchase Order amount do not match, the Financial Management Analyst will contact the signer to resolve.

d. When vendor invoice is received the quantity and price should be compared to original order.

e. No payments should be made before actual receipt of item.

f. Payments to vendors should be made promptly.

g. Contracts should be monitored to ensure that maximum obligation is not exceeded or that sufficient time is provided for approved modifications.

9. Payroll/Personnel

a. The GBCVB uses ADP for payment of the bi-weekly employee payroll.

b. An employee can only be placed on the payroll when there is a properly submitted approval/authorization form.

c. All employees are required to document their attendance.

d. All weekly attendance records are transferred to a time log system maintained by the Human Resources Department.

e. The Financial Management Analysts will reconcile and verify the biweekly payroll before issuance of the checks. The final approval is done by Senior Vice President of Administration or the President.

f. The Director of Finance maintains all employees W-4 withholding allowance and forms.

g. No voluntary deductions (i.e. direct deposit, insurance deductions, and 401K deductions) will be initiated or terminated without written authorization of the employee. The appropriate documentation must be maintained by the Director of Finance.

h. All reconciled payroll documents must be approved by pay period along with supporting documentation.

10. Cash Reports

a. Checks received must be properly endorsed with 'deposit' only.

b. Cash and check receipts should be deposited on a daily basis by the Account Receivable Coordinator.

II. Security

a. Department Directors Signature Authorization

Each department director is responsible for their budget, all activities conducted by the department, and for setting up the departments operations with a series of checks and balances to balance risk and efficiencies.

b. Security of Records

Senior management must ensure the security of records and data in hard copy or electronic format. The GBCVB has set up measures to assist in preventing threats from within as well as outside the organization including a secure fax machine for processing credit card payments. The GBCVB has adopted and has in place a Written Security Information Program in place.

c. System Security

Senior management determines each employee's individual security access. We have also set up safeguard procedures for specific areas such as accounts receivable, payroll, purchasing, computer and building access as well as the appropriate security level for each. The GBCVB has adopted and has in place a Written Security Information Program.

d. Data Security

Data security is the means of protecting data against unauthorized disclosure, transfer, modification or destruction whether accidental or intentional. Data security ensures privacy, protects confidential data on employees, members and stakeholders. The GBCVB has set up procedures and policies that prevent unauthorized access to computer resources and include:

- Level of system access is defined for all employees;
- Password safeguards are in place with periodic changes of passwords;
- Each user has a unique ID;
- Limited number of users access to system software;
- Control access to specific applications and data files;
- Review of security logs;
- Adequate virus protection procedures implemented;
- Lock installed on Server room door;
- Access to systems reviewed quarterly and when turnover occurs in sensitive positions or realignment of responsibilities;
- iphones, iPads have email remote wipe capability through MS Exchange.

e. Physical Security

- Protection of personnel and records and all assets from fire, natural disasters, burglary, theft, vandalism and terrorism are all part of physical security. The GBCVB has set up a number of procedures to assist in its security effort including:
- Key personnel with sensitive record information must lock their office nightly;
- Server room locked;
- Keyless office door entrance with code access changed regularly;
- All employees must show Building issued ID badges for access;
- All guests must show picture ID for building access to security personnel;
- Logs are kept by building management office and are available for GBCVB's review;

- Quarterly fire drills are conducted by Building management and public announcement system is in place for notification of building issues or closures;
- Building has an information system in place to notify tenants of building closures or issues which is then shared with our employees through our email/phone systems;
- Daily backups to offsite location with 5 generations of files;
- The GBCVB has adopted and has in place a Written Security Information Program,

MONITORING:

The purpose of monitoring is to determine the effectiveness of internal controls in order to ensure that the controls reflect the current environment are adequately designed, properly executed and effective. The GBCVB monitors its internal controls policies and procedures as set forth in this Plan. This monitoring is accomplished through continuous review and updating of the internal controls policies and procedures and evaluation of systems.

All employees need to understand the GBCVB mission, goals, objectives, risk levels and their own responsibilities. Everyone in the organization shares the responsibility for monitoring.

On site audit reviews are performed annually by an independent certified public accountant firm. Senior Management is notified of any irregularities or inconsistencies identified in the process. The annual audit is submitted to the Finance Committee and then to the Board.

The Senior Management is responsible for updating and/or amending the GBCVB's internal control policies and procedures. The Senior Management and Human Resources Department are responsible for ensuring adequate training and communication for staff.

INFORMATION AND COMMUNICATION:

Information and communication is the means by which risks, policies and procedures are shared with the staff, members and stakeholders. GBCVB recognizes that information must be communicated to staff at all levels, in all directions as well as to our stakeholders and members in a timely manner. Monthly e-newsletters are sent to members and stakeholders and the Finance Committee, Executive Committee and Board of Directors meet regularly and minutes of the meetings are distributed. Reports are submitted by Senior Management relaying pertinent information regarding their department's goals status. This information is shared with the Board of Directors at Board Meetings. External

communications also used to include press releases, newsletters to members and stakeholders, the GBCVB's web site, publications and social channels.

RISK ANALYSIS – SUMMARY OVERVIEW:

A GBCVB Risk Analysis was performed on the potential risks that could prevent the GBCVB from reaching its goals and adhering to its mission. The risks identified by senior staff are listed below. In response to the list the GBCVB has evaluated the significance of each risk identified, the likelihood of it happening, and what measure must be taken or planned to help minimize the effects. The GBCVB staff considered how they wanted to handle the risks by identifying steps that need to be taken. There are other potential risks that are not included because individually they do not meet this higher risk level standard.

AREAS OF RISKS AND THEIR CORRELATION TO THE GBCVB'S GOALS

ITEM 1: OVERALL MEMBER FUNDING

Area of Risk:

- Sufficient funding from our members is necessary to operate and maintain staff and programs, maintain staffing levels and programs and meet the GBCVB's contractual obligations to match at least every public dollar with a private sector generated dollar.

Potential Risk if not addressed:

- Inadequate funding levels could cause cutbacks in programming and initiatives that will reduce our ability to meet our mission and goals.

Corrective Steps to be taken:

- Follow industry best practices for membership retention and services circulate to all staff monthly status reports.

Steps Already Taken:

- A membership development and retention program is developed yearly and results tracked.
- Prepare and submit a budget that outlines a spending plan that obtains approval for the allocation of appropriated funds. Budget is approved annually by Board and noted in minutes.

- Ongoing review of budget on a monthly basis including both revenue and expenses and financial statements are provided each month to Department Directors for review.

Responsible:

President & Senior Staff, Finance Committee, Executive Committee and Board.

ITEM 2: LEGISLATIVE FUNDING

Area of Risk:

- Dramatic reductions or elimination altogether of the State Legislature's funding of Regional Tourist Councils.

Potential Risk if not addressed:

- A significant reduction and/or elimination of Legislature's funding for 1038 marketing grants will result in significant programmatic cutbacks and staff reductions leading to inability to carry out our mission.

Corrective Steps to be taken:

- Develop and identify alternative funding models and sources for both the short term and long term.

Steps Already Taken:

- An Operating Reserves Accounts has been created.
- An Operating Reserves policy has been established which requires that yearly GBCVB set a goal of having an Operating Reserves Account that represents 25% to 50% of the GBCVB's total budget minus the MCCA contract amount.

Responsible:

President & Senior Staff, Finance Committee, Executive Committee and Board.

ITEM 3: EFFICIENT ORGANIZATION MANAGEMENT

Area of Risk:

- The GBCVB needs to update and in some cases create policies and procedures for monitoring, supervising and evaluating its programmatic and fiscal operations**.**

Potential Risk if not addressed:

- Without updated policies and procedures for the organization, the possibilities of errors, irregularities, fines, miscommunication and goals and objectives not being met is greatly enhanced.

Corrective Steps to be taken:

- Updating and adding policies and procedures for the employees, and operations of the organization.
- Development of a timeline for training employees to implement these policies and procedures.
- Develop a Succession Plan for Senior Staff by requiring each Director to identify candidates with skill set necessary to fill their position.

Steps Already Taken:

- Internal Control Plan written.
- Ongoing evaluation of Internal Control Plan.
- Specific controls for new or special programs developed and documented.
- Procurement Policies and Procedures written, approved and distributed.
- Periodic reviews of program Policies and Procedures.
- Ongoing meetings of Senior Management held to develop Risk Assessment topics.
- Periodic review of existing policies and procedures for changes needed due to internal and external forces.
- Written Information Security Program adopted.
- General Data Protection Regulation (GDPR) addendum, as it relates to email subscriptions and web visitation, integrated with privacy policy on website.

Responsible:

President & Senior Staff

ITEM 4: INFORMATION AND TECHNOLOGY SECURITY

Area of Risk:

The GBCVB needs to maintain a high level of data and hardware security to protect against abuse and misuse of their computer systems including:

- Access to servers, routers and firewall.
- Hardware failure from environmental factors.
- Unauthorized employee access.
- Lack of backup personnel.
- Virus, DOS attacks.
- Backup data in the event of system failure or catastrophe.
- Endpoint Security.

Potential Risk if not addressed:

- Physical abuse and unauthorized access to computer files.
- Overheating and shutdown of equipment.
- No personnel to manage computer systems, unable to access systems, unknown administrator passwords.
- Inappropriate data sharing.
- Unauthorized access to computer files, corruption and theft of data.
- Hardware system failure or software corruption.
- Data (CRM, CMS, email) not accessible.

Corrective Steps to be taken:

- Limited Server Room access.
- Adequate ventilation installed.
- Frequent password change.
- Procedure to notify of terminated employee, intern or contractor.
- Identify and train backup personnel or contractor.
- Current Virus Software on all systems.
- Daily data backups.
- Offsite storage with redundancy
- Ability to remote wipe mobile endpoints.
- A secure fax machine for processing credit card payments.

Steps Already Taken:

- Lock installed on Server room door.

- New ventilation installed to meet the needs of the server room equipment heat loads.
- Automatic password changes required every 90 days.
- Social Media Usage policy updated and added to the new employee orientation and shared with existing employees.
- Email moved to the cloud.
- Phone system moved to the cloud – phones can be used anywhere there is high speed internet access.
- CRM and CMS hosted offsite by vendor – vendor has redundant servers in multiple locations.
- Installed cloud-based virus and spyware software on all computers. Centrally managed site with automatic virus definitions sent to all machines.
- Daily backups to offsite location with 5 generations of files.
- iPhone, iPad have email remote wipe access through Exchange.
- Written Security Information Program adopted.

Responsible:

iCorps with Vice President of Operations and Operation Manager.

ITEM 5: ANTITRUST

Area of Risk:

- Antitrust violations.

Potential Risks if not addressed:

- Violation of federal or state laws will have criminal or civil penalties.

Corrective Steps to be taken:

- Annual recording in Board minutes that Board Members have discussed antitrust responsibilities and been advised not to violate antitrust laws in their actions as GBCVB Board members.

Steps Already Taken:

- A policy of Antitrust avoidance has been created and distributed.
- Board members sign and submit a Conflict of Interest and Antitrust Compliance forms annually.

Responsibility:

President, Senior Staff and Board.

ITEM 6: UNRELATED BUSINESS INCOME TAX

Area of risk:

- In any given year, the GBCVB could generate significant advertising income from its publications which would trigger unrelated business income tax liability.

Potential Risks if not Addressed:

- IRS audit and findings of unrelated business income could result in additional taxes and penalties which will create a financial burden on the organization.

Corrective steps taken:

- GBCVB Finance Director has been responsible for doing this analysis and then preparing 990T form required by IRS.

- To ensure broader compliance and timely completion of the unrelated business income form, we have hired an independent outside tax consultant and firm to prepare our overall Tax Form and the 990T Form.

Steps Already Taken:

- Tax Form is reviewed by the GBCVB Finance Committee of the Board and approved by the Board.

Responsible:

President, Senior Staff, Finance Committee and Board.

ITEM 7: USE OF SOCIAL MEDIA

Area of Risk:

- Social media applications pose potential security risks to the organization and GBCVB can be liable for any social media it controls and can result in lawsuits and member resignations.

Potential Risk is not addressed:

- Confidential or privileged information is shared through social media. Social media applications can pose potential security risks – i.e. a code that could damage the organizations computer network.

Corrective steps to be taken:

- Guidelines and controls for social media content, copyrighting and professionalism have been established and will be added to the list of new employees' Agreement Forms.
- Regularly reminding employees that the organizations reputation in the community is everyone's responsibility.

Steps Already Taken:

- Created Social Media Usage Policies Guide and distributed to employees.
- Organization's rules prohibit discrimination, harassment, and threats of violence apply to both verbal and on-line communications.

Responsible:

Sr. Vice President of Administration and Sr. Web Marketing Manager

ATTACHMENTS

GBCVB BOARD AGREEMENT

The following guidelines have been established regarding the level of participation that is required for all Board members of the Bureau:

BOARD RESPONSIBILITIES AND STANDARDS

Position Description for Board Members:

I. **General Responsibilities:**
The Board is accountable for the GBCVB's continued viability and accomplishment of its mission. Towards these ends, a Board member:

a. Reviews and approves GBCVB's mission and long-term strategy;

b. Reviews and approves GBCVB's policies pertaining to finance, internal controls, human resources, collections management and other significant areas;

c. Reviews and approves annual and long-range financial plans including annual audit;

d. Holds the President accountable for planning and delivering GBCVB programs and initiatives;

e. Carries out operational functions in governance, such as adopting by-law changes, nominating and selecting officers, Board Members and evaluating Board performance;

f. Assures the GBCVB fulfills all legal requirements and obligations.

II. Performance Standards for Board Members:

a. Board members must be current dues paying members of the Bureau;

b. Serves on at least one committee;

c. Participates in at least three-quarters of Board meetings and a majority of committee meetings, whether in person, over the phone or electronically;

d. Board members must recommend two new member prospects each year;

e. Board members must attend at least one of the member Open House meetings;

f. Come to meetings prepared to ask informed questions, and make a positive contribution to discussions;

g. Respects the confidentiality of the Boardroom;

h. Carries our his/her responsibilities in recognition of fiduciary responsibility to the GBCVB;

i. Disclosures to the Board any potential conflict of interest and removes himself/herself from discussion where a potential conflict exists. Completes and submit an annual Conflict of Interest Statement;

j. Understands the antitrust requirements and avoids any situations that could trigger antitrust actions and completes and submit an Antitrust Compliance form annually.

GBCVB PROCUREMENT POLICY

ROLES AND RESPONSIBILITIES

All Greater Boston Convention & Visitors Bureau (GBCVB) staff is responsible for ensuring that procurement activity within their program area is carried out in accordance with the Acquisition Procedure.

1. ACQUISITION PROCEDURE

The GBCVB will conduct all procurement transactions in a manner that maximizes opportunities for membership and increases the quality of purchase. The GBCVB reserves the right to reject any bids or offers, if deemed to be in its best interest.

2. PRICING PROCEDURE

The following procurement procedures shall be utilized for all purchases of equipment, materials, supplies, property, or services involving amounts over $500. A purchase order must be submitted to the Financial Management Analyst for any purchase over $500 or any credit card purchase regardless of amount size in advance of the transaction. All procurement using state or federal funds shall be in compliance with the terms of the contracts signed for these funds.

3. OPEN MARKET INQUIRIES

In the case that there is not a member suitable for the goods/services, the GBCVB may request services outside of membership, in hopes that the vendor will become a member.

4. REQUESTS for COMPETITIVE QUOTES

The GBCVB may request competitive quotes, orally or in writing, from at least three different sources. The file (electronic or paper) shall document each request made and offer received, especially in procurement of goods/services in excess of $3,000. The lowest priced vendor will not necessarily be chosen as we desire to spread opportunities across the current membership of the GBCVB.

5. DOCUMENT PRICES

The GBCVB shall maintain files on all quotations solicited and offers or bids received and any criteria for selection. In all instances in which the lowest bid is not awarded in the contract, justification for the selection must be contained in the file.

The President and Sr. Vice President of Administration must approve expenditures over $25,000.

GBCVB VENDOR MANAGEMENT POLICY

To manage the selection of new vendors and to assess the ongoing performance of certain existing vendors, this document shall serve as a guideline for best practices.

VENDOR RISK RATING

High Risk

A vendor that provides services critical to the normal daily operations, with or without access to private member or employee information, without which the GBCVB would be significantly disadvantged, and the vendor cannot be replaced without unacceptable disruption and or substantial financial and or labor cost.

Medium Risk

A vendor that provides services that are critical to normal daily operations, but the vendor is replaceable without significant disruption and without significant labor or financial costs.

A vendor is not critical to normal daily operations but maintains processes or otherwise has access to member or employee personal information in the course of providing services to the GBCVB.

Low Risk

All other vendors, who do not meet the criteria for high or medium risk, including those who can be easily replaced with little financial or labor cost to the GBCVB. Vendors without which the GBCVB would not be hindered from providing daily services to members, customers and employees and who do not have access to non-public information or personal information.

VENDOR SELECTION & DUE DILIGENCE

Responsibility for selection and administration of each vendor relationship is assigned to personnel with appropriate expertise to monitor and manage same.

I. Initial Considerations & Due Diligence

A. Assessment of the vendor's experience and adequate industry knowledge consistent with the needs of the GBCVB. Assure the vendor has sufficient relative experience, demonstrated by prior assignments of similar nature.

B. Assessment of technical knowledge capable of completing the required assignment. The relevant staff will ensure that the vendor's staff has requisite technical knowledge capable of completing assignments in a timely and proficient manner.

C. Assessment of operational controls. The relevant staff will assess the controls to ensure they are sufficient to maintain security and confidentiality of the information assets of the GBCVB and its members. This assessment may include an onsite visit. Vendor must be willing to comply with all stipulations

to which the GBCVB is subject, such as grantor restrictions.

D. Assessment of business continuity planning. For high and medium risk vendors, the relevant staff will obtain assurances from the vendor that it has implemented a disaster recovery plan and or continuity plan and testing if available.

E. Financial Condition of the vendor. For high and medium risk vendors, the relevant staff will assess financial condition of the vendor to ensure ongoing viability.

F. Insurance. Obtain evidence of the vendor's insurance policies and determine whether the coverage is sufficient.

II. Ongoing Due Diligence & Periodic Review.

A. After engagement, each high and medium risk vendor will be periodically reviewed by the relevant staff or qualified designee to assess the performance and adequacy of controls.

B. High risk vendors will be reviewed annually, and a report made to the GBCVB Board of Directors.

C. Medium risk vendors will be reviewed every 24 months or earlier if there is an event such as a significant increase in services, unsatisfactory performance, change in ownership, or awareness of operational/financial trouble.

III. Review Criteria.

A. Description of product/service;

B. Assessment of quality of service & support;

C. Assessment of financial condition & operations;

D. Changes in Corporate structure;

E. Disaster recovery plan / results;

F. Information, security programs;

G. Review of contract compliance and revisions;

H. Review of liability insurance coverage;

IV. Contract Provisions.

A. Scope
   a. Timeframe;

b. Frequency, format, specifications of service or product provided;

c. Other services provided (support, maintenance, training, customer service);

d. Compliance with applicable laws, regulations:

e. Authorization for the GBCVB to have access to records as are necessary or appropriate to evaluate compliance with laws;

f. Identification of which party is responsible for delivering any disclosures;

g. Insurance maintained by vendor;

h. Terms relating to use of GBCVB premises, equipment or employees;

i. Permission/prohibition of vendor to subcontract to another party to meet its obligations, subject to any notice/approval requirements and opt out language allowing the GBCVB to terminate the contract should the vendor not disclose use of subcontractors;

j. Authorization for the GBCVB to monitor and review the vendor for compliance with the parties' agreement.

B. Cost/Compensation

a. Outline the fees to be paid, including fixed compensation, variable charges and any fees to be paid for nonrecurring items or special requests. Also address cost and responsibility for purchasing and maintaining equipment, hardware, software or other item related to the activity. Also, the party responsible for payment of any legal or audit expenses should be identified.

C. Performance Standards

a. Clearly defined performance standards included as a basis for performance measurement, and may also be used as a factor in compensation arrangements;

D. Reports

a. Specify type and frequency of management information reports to be received from the vendor.

E. Audit

a. Specify the GBCVB's right to audit the vendor (or engage an independent auditor to do so).

F. Confidentiality & Security

   a. Contract should prohibit the vendor and its agents from using or disclosing the GBCVB's information, except as necessary to perform the functions designated in the contract. Nonpublic information must be handled consistent with privacy laws.

G. Customer Complaints

   a. Specify whether the GBCVB or vendor has duty to respond to any complaints received from members or customers. If it is the vendor, the GBCVB should receive a copy.

H. Business Resumption & Contingency Plans

   a. Specify the vendor's responsibility for continuation of services in the event of an operational failure, including manmade and natural disasters. Vendor should have appropriate backup of information and recovery plans.

I. Default & Termination

   a. To mitigate risk with contract default or termination, the contract should address both issues. Specify what circumstances constitute default, identify remedies and allow for reasonable opportunity to cure a default. Termination rights should be identified in the contract, especially for material vendor arrangements and rapidly changing technology or circumstances;

   b. Termination rights may be sought for change in control, substantial increase in cost, failure to meet performance standards, failure to fulfill contractual obligations, inability to prevent violations of law, bankruptcy, company closure and insolvency. Contract should state termination and notification requirements and operating requirements and time frames to allow for orderly conversion to another vendor without excessive expense. Return of GBCVB data, records and other resources should be addressed.

J. Dispute resolution

   a. Consider a resolution process.

K. Ownership & License

   a. Address ownership issues and vendor's right to use GBCVB property, including data, equipment, photography, software, magazine content;

   b. GBCVB name and logo and other copyrighted material. Address ownership and control of any records generated by the vendor.

L. Indemnification

   a. Require the vendor to hold the GBCVB harmless from liability as the result of negligence by the vendor and vice versa.

M. Limits on Liability

   a. A vendor may wish to limit the amount of liability it could incur as a result of the relationship with the GBCVB. Consider whether the proposed damage limitation is reasonable compared to the loss the GBCVB could experience should the vendor fail to perform.

SOCIAL MEDIA USAGE AND POLICIES

GBCVB SOCIAL MEDIA POLICY FOR EMPLOYEES

Guidelines for functioning in the digital world are the same as the values, ethics and confidentiality policies

*GBCVB **employees** are expected to follow every day.*

- GBCVB employees are perceived representatives of the Bureau, even during non-working hours. As an employee, you should exercise good judgement when using electronic media. Protecting the Bureau's reputation in the community is every employee's responsibility;
- Employees should understand that nothing is anonymous on the Internet;
- Employees should understand that electronic communications using the Bureau's computers are not confidential or private, and may be accessed by the Bureau at any time;
- The Bureau has the right to access any data and information regarding the Bureau from an employee's public social media tools, even if the data resides in off-site servers;
- Employees shall not disclose any confidential or privileged information about the Bureau or employees through social media;
- Employees should not imply or state that they represent the views of the Bureau (except where assigned by Management to do so as part of their job) and must clearly represent that their views are their own. Employees may not post information that may reflect negatively on the Bureau (unless protected by law);
- The Bureau's rules prohibiting discrimination, harassment, and threats of violence apply to online communication as well as verbal communication;

The GBCVB communicates through and monitors the following social media channels:

- Facebook
- Twitter
- Pinterest
- Instagram
- YouTube
- Blog

FACEBOOK

The Greater Boston Convention & Visitors Bureau (GBCVB) maintains a Facebook page under the name BostonUSA where we share valuable visitor and local information as well as deals and events in the

city. We respond to comments and messages in a timely manner and always assist whenever possible. We encourage a high level of engagement from our community, visitors and member companies. Our Facebook page is managed by various staff members of the GBCVB.

TWITTER The GBCVB raises awareness and informs the public about various key information and events in the city through our Twitter account, @visitboston. We engage our local and visitor audience through this account by answering questions, giving suggestions or simply informing the public.

PINTEREST

The GBCVB maintains and continually adds new content/boards to our Pinterest account, pinterest.com/bostonusa. We interact with potential visitors as well as our local community with a variety of boards.

INSTAGRAM The GBCVB manages an Instagram page, instagram.com/visitboston and we encourage interaction by use of our hashtag (#BostonUSA) which allows visitors and locals alike to share their images/experiences in Boston. Use of this hashtag provides the Bureau with permission to 'regram', or re-post.

YOUTUBE

The GBCVB manages a YouTube account under the name GBCVB - youtube.com/gbcvb. We publish our video content to this website.

VIMEO

The GBCVB manages a Vimeo account under the name GBCVB - vimeo.com/gbcvb. We publish our video content to this website, as well.

HUBA HUBA BLOG

The GBCVB manages a blog, and we encourage visitors and locals to visit the blog and comment/subscribe to the blog for valuable information.

GBCVB SOCIAL MEDIA POLICY FOR OFFICIAL ACCOUNTS

*Guidelines for functioning in the digital world are the same as the values, ethics and confidentiality GBCVB policies **official social media administrators** are expected to follow every day.*

Best Practices

- Tone and messages are upbeat and welcoming to reflect the job role of a destination ambassador.
- When borrowing content from an external source, credit the source (i.e. artist, photographer, etc.)
- Passwords should be updated bi-annually, and follow a two-factor authentication.
- On Instagram, GBCVB uses 'regrams' as part of a user-generated media strategy; we re-post photos from another user's account if they tag their media with our established hashtag: #bostonusa

Social media representatives are prohibited from disseminating messages that contain:

- Profanity and vulgar or abusive language;
- Threats of physical or bodily harm;
- Sensitive information (for example, information that could compromise public safety);
- Offensive terms that target specific ethnic or racial groups;
- Reproduced or borrowed content that reasonably appears to violate third party rights.

USE OF GBCVB LOGO, TITLES, GRAPHIC ELEMENTS

All graphic elements of GBCVB logos, events and products shall be copyright protected, and trademark protected as allowed by state and federal law.

I. GBCVB logo

II. GBCVB titles of programs such as **Dine Out Boston;**

No use of the GBCVB logo or product / program names or editorial content from websites and magazines shall be allowed without permission of the President & CEO or Board of Directors.

Unauthorized use of the GBCVB name, logos, titles, graphic elements shall not be construed as an endorsement of the Greater Boston Convention & Visitors Bureau.

BostonUSA letterhead and/or logo will not be used for political fundraising or personal use of staff, volunteers or members. Unauthorized use of the letterhead/logo will result in a verbal warning, written warning or immediate dismissal.

GBCVB ANTITRUST COMPLIANCE POLICY AND GUIDELINE

It is the policy of the Greater Boston Convention & Visitors Bureau ("GBCVB" or "the GBCVB") to comply with all antitrust and competition laws. The fundamental objective of the antitrust laws is to protect and promote free and fair competition. These laws reflect the belief that a competitive marketplace will enable consumers to obtain the highest quality goods and services at the lowest price. The GBCVB supports the public policies embodied in these laws, and it is the association's policy to comply fully with them.

Through the adoption and issuance of the GBCVB Antitrust Compliance Policy and Guidelines (the "Policy"), the GBCVB affirms its commitment to abide by the spirit and the letter of all antitrust laws. All members of the GBCVB and their representatives must follow the policy and guidelines contained herein as part of their ongoing obligations to the GBCVB. The Guidelines are intended to provide basic guidance on the antitrust laws which may be applicable to the activities of the GBCVB. Counsel should be consulted in all cases involving specific situations or interpretations.

This Antitrust Compliance Policy and Guidelines provides a brief overview of some of the more common antitrust issues that may arise as a result of your affiliation with the GBCVB. The goal is not to provide a comprehensive explanation of the antitrust laws or to make you an expert in the area. Rather, the Policy is intended to help you recognize the kinds of conduct that the antitrust laws address and to enable you to identify when you should seek legal advice. Whenever you have any questions about the possible application of the antitrust laws to any of your activities, you should consult legal counsel for the GBCVB or or your own legal counsel who has responsibility for considering the antitrust implications of the business activities in question.

I. OVERVIEW OF THE ANTITRUST LAWS

The antitrust laws are based on the fundamental assumption that a competitive process will increase the supply and reduce the price of goods and services. These laws therefore prohibit conduct that will unreasonably restrain competition or restrict the freedom of action of businesses in their respective operations. The pro competitive purposes of standard-setting bodies have long been recognized. Still, because Forums such as the GBCVB gather competitors together, they are susceptible to certain antitrust pitfalls, and thus frequently are scrutinized by antitrust agencies. As such, the GBCVB must operate with heightened sensitivity to antitrust laws.

Sherman Act, § 1. The most important antitrust law applicable to the GBCVB is Section 1 of the federal Sherman Act, which prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade." Although this prohibition might seem to encompass almost every business transaction, the courts and antitrust agencies have interpreted it so that only restraints that are "unreasonable" are forbidden. Some agreements by competitors are deemed so harmful and facially unreasonable that they are considered *per se* illegal. This means that they cannot be justified by arguments about the reasonableness of the prices charged or the need to avoid chaos in the marketplace. These generally include agreements among competitors to fix prices, to reduce price competition by allocating customers, territories or markets, certain "tie-in" sales, and some forms of boycotts. The government may prosecute violations of Section 1 criminally or civilly. Violations of Section 1 are also frequently the subject of private civil damage suits.

Section 5 of the Federal Trade Commission Act. Another law that frequently is applied to the conduct of trade associations and standard-setting bodies is Section 5 of the Federal Trade Commission Act. Section 5 prohibits "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." The provisions of the FTC Act can be applied to a company acting alone (unlike Section 1 of the Sherman Act) and are written more broadly than the provision of the Sherman Act.

State Laws. It is also important to recognize that state antitrust laws may be applicable to certain GBCVB activities. These laws generally parallel the provisions of federal antitrust law. Because these Guidelines cannot catalog each state law, appropriate counsel should be consulted if any questions arise as to the propriety of actions conducted in a particular state.

II. AGREEMENTS AMONG COMPETITORS ("HORIZONTAL AGREEMENTS")

A. What is an agreement? It is not necessary for an agreement to be formal or memorialized in writing for it to constitute an antitrust violation. A court may find there has been an illegal "agreement" under the antitrust laws even though there is no written contract, no "handshake," and no words that indicate an explicit agreement. An agreement may include informal, unwritten, and even unspoken agreements or understandings. In addition, illegal agreements can be established by circumstantial evidence, such as a pattern of conduct or mere presence at a meeting at which illegal agreements were made.

In fact, competitors may be accused of making illegal agreements even though there are no direct communications at all. If, for example, a price increase is announced well in advance of the effective date, it may sometimes be argued that the announcement was a “signal” to competitors that invited an agreement to take similar action.

From a practical standpoint, GBCVB members should focus their concern on the following antitrust violations that may arise pursuant to competitor agreements:

B. Price Fixing. It is not always easy to recognize what is and what is not price fixing. Any agreement among competitors to raise, lower or stabilize prices is unlawful, even if the agreed-upon price is reasonable, and even if the agreement is never put into effect. Details like credit terms, discounts, and warranties are an element of price. Competitors may be charged with illegal price fixing if they discuss general pricing ranges or policies because these discussions may have an impact on actual price quotations.

C. Market Allocation. Agreements among actual or potential competitors to allocate customer, territories, or lines of business also are usually serious antitrust violations because they reduce or eliminate price competition. Thus, it is illegal for two competitors to agree that one of them will not sell in a particular territory or to a particular customer that they both can presently serve. Similarly, it is unlawful for them to agree on the type of services or products that they will offer to customers.

It may not be an illegal allocation, however, if these limitations are contained in intellectual property licensing agreements because such licensing arrangements may be more pro-competitive than an alternative scenario in which no licenses are granted at all.

Similarly, allocation of customer, territory, or line of business responsibilities in connection with a joint venture among actual or potential competitors may also be permissible because that division of roles is reasonably necessary for the joint venture to achieve efficiencies or produce better products and services that benefit consumers. Legal advice is needed in these situations.

D. **Group Boycotts**. A collective refusal by otherwise competing companies to deal with some third party, sometimes called a "group boycott," raises serious antitrust concerns. It is dangerous for one company to agree with another company that neither one will do business with a particular supplier or customer, or that they will do business only with certain suppliers or customers or only on certain terms and conditions.

Agreements between Suppliers and Customers ("Vertical" Agreements)

Agreements with suppliers and customers (other than those relating to resale prices) usually are legal unless some anti-competitive effect can be demonstrated. Moreover, these agreements can often be justified on the ground that they are reasonable. Such agreements are also far more likely to be embodied in specific written contracts, rather than inferred from discussions, so there is less risk that ambiguous conduct will be misunderstood.

The following kinds of "vertical" agreements are most likely to raise legal questions, and therefore prior consultation with GBCVB counsel or your counsel is essential.

A. **Exclusive dealing or requirements contracts**. A contract may provide that one company will deal exclusively with a specific seller or buyer. These agreements may preclude the supplier's competitors from participation in the business under contract. The legality of these arrangements depends on a variety of factors. In general, a contract for a short period of time, such as one year or less, does not raise antitrust concerns. Longer contracts may raise problems depending on the market shares involved and the business justification.

B. **Preferential treatment**. The sale of the same goods to different customers at different prices raises a legal question, as do agreements to favor certain customers in promotional programs. There may be available justifications, but advice is required because there are a lot of technical distinctions.

   It is usually safe to enter into a "most-favored-nation" contract, which guarantees that no other customer will be treated more favorably than the contracting customer. On the other hand, there can be a problem if a contract guarantees that the contracting customer will get better treatment than anyone else.

C. **Tying arrangements and reciprocity**. There may be a problem when a company attempts to extend whatever power it may possess in some segments of its business (the "tying" products) into other segments of its business (the "tied" products).

   On the other hand, it is not illegal to package the sale of goods or services at a particularly favorable price — so long as the customer has the realistic choice of purchasing the

individual goods or services separately.

Reciprocity differs from tying in that the seller of one product or service is the buyer of the other. The difference between illegal reciprocity and legal commercial relationships is difficult and legal advice is necessary.

D. Resale price restrictions. Unlike other "vertical" contracts, agreements with customers on the prices that they will charge to their customers are almost invariably illegal. Even agreements which appear to place a ceiling on resale prices can raise serious antitrust questions.

Antitrust Guidelines

Any implication of collusion arising out of GBCVB activities must be avoided at all costs. Some ways to do this are to avoid specific discussion of prices or any of the elements of pricing, such as pricing policies, discounts, warranties or guarantees, terms or condition of sale, credit, shipping, or commercial liabilities. Discussion of general elements of prices, such as saying that including something may be too expensive or that the benefits may outweigh the costs, is allowable. Above all, do not exclude or control competition. All parties have a right to be heard under the principle of openness.

In order to minimize the antitrust risks associated with standards setting activities, the following guidelines should be followed regarding both the development and adoption of a standard as well as the promulgation of that standard:

I. Discussions in all GBCVB related meetings, including Board and Working Group meetings, should relate solely to the legitimate purposes of GBCVB. Care should be taken to avoid even the appearance of discussing competitively sensitive information, as such discussions may lead to the inference of an illegal agreement on prohibited topics. To this end, there should be no discussion, communication or other exchange between members of the GBCVB and/or their representatives regarding any of the following categories of information:

1. Prices or pricing strategy. This requirement is to be interpreted broadly, to include, for example, current or projected prices; price levels; pricing procedures or formulas; price changes or differentials; markups; discounts; allowances; terms and conditions of sale, including credit terms, warranty provisions, etc.; or other information that might comprise an element of a product's price, including profits, margins or cost data;

2. Production levels, production capacity, or product inventories;

3. Plans pertaining to the development, production, distribution, marketing, or introduction dates of particular products, including proposed marketing territories and potential customers;

4. Terms on which any GBCVB members will or will not deal with particular competitors, suppliers, distributors, or customers;

5. Current or projected cost of procurement, development, or the manufacture of any product;

6. Allocation of customers, markets or territories;

7. Non-public information regarding market shares.

II. GBCVB membership should be available to all interested businesses and organizations on reasonable terms. No applicant for membership, who otherwise meets the qualifications set forth in the Bylaws of the GBCVB, should be rejected for any anti-competitive purpose or solely for the purpose of denying such applicant the benefits of membership.

III. Special care should be taken to ensure that no GBCVB meeting is used as a means of violating the terms of this Policy. Accordingly, the following practices should be followed:

1. All meetings should follow a written agenda. If potential antitrust questions are raised by an agenda item, such item will be reviewed in advance by counsel;

2. The Board Secretary should prepare minutes promptly after the meeting, summarizing all matters discussed. Only minutes approved by the Board and/or counsel should be distributed (even in preliminary form) and only minutes as approved need be retained. The purpose of this is to avoid the preservation of misstatements and ambiguities that may create misperceptions of the meeting. All Board minutes will be made available on a timely basis.

3. Informal meetings should not be held and informal discussions should comply with the standards of this Policy.

IV. Members shall not discuss the degree to which members will or will not do business with firms that do not participate in the GBCVB.

V. Any information, materials, or reports of the GBCVB available for the use of its members should be made available to non-members on reasonable terms when non-availability of those materials imposes a significant economic disadvantage or cost to nonmembers that significantly limits their ability to compete against GBCVB members. Once a specification is adopted, it should be made available to members and non-members on payment of reasonable fees. In addition, related manuals and services necessary to implement the specification should also be made available.

III. CONCLUSION

As the foregoing discussion sets forth, activities of the GBCVB will not include any actions that violate the law. The GBCVB, in the course of its activities, shall not agree with, participate in, or give consideration to any activity, plan, understanding, agreement, or other arrangement that constitutes a violation of any federal or state antitrust laws, including but not limited to actions that would (a) raise or stabilize prices or fees, (b) boycott or refuse to do business with any third parties (other than through the GBCVB's bona fide business contractual arrangements), (c) restrict or interfere with the exercise of free and independent judgment by the members in the management or operation of their respective business, or (d) obstruct or interfere with commerce or free and

lawful competition. Members of the GBCVB shall conduct all activities in compliance with the GBCVB's Bylaws and this policy on compliance with the antitrust laws.

You should consult with GBCVB staff and/or legal counsel for the GBCVB when you are in doubt about the legality of any business activity. Even if the Antitrust Policy and Guidelines do not seem to apply literally, such consultation should occur whenever any proposed activity strikes you as "unfair," overreaching, or likely to be challenged by another party. Until you have received affirmative clearance for a proposed course of action that has raised doubts in your mind, do not do it.

GBCVB INFORMATION SECURITY PROGRAM

1. OVERVIEW AND PURPOSE

The Greater Boston Convention and Visitors Bureau ("**GBCVB**") has adopted this written information security program (the "**Information Security Program**") in an effort to better safeguard Personal Information that it may collect, store or maintain in its Records. This Information Security Program is designed to: (i) protect the security and confidentiality of Personal Information in a manner fully consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of Personal Information; and (iii) protect against unauthorized access to or use of Personal Information in a manner that may result in substantial harm or inconvenience to any customer, employee or member.

This Information Security Program is intended in good faith to comply with Title 201, Section 17.00 of the Code of Massachusetts Regulations ("**Regulation 201**"), and it applies only to the extent required by law. GBCVB reserves its right to challenge the validity and enforcement of Regulation 201 as applied to GBCVB, and this Information Security Program shall have no force or effect if it is later determined that Regulation 201 does not apply to GBCVB.

GBCVB has developed this Information Security Program in light of: (i) the size, scope and type of activities in which it is engaged, (ii) the resources available to it, (iii) the amount of data it stores; and (iv) the need for security and confidentiality of its employees, customers and members. GBCVB has also taken into consideration the materials published by the Massachusetts Office of Consumer Affairs and Business Regulation, including its: (a) Small Business Guide for Formulating a Comprehensive Written Information Security Program, (b) 201 CMR 17.00 Compliance Checklist; and (c) Frequently Asked Questions Regarding 201 CMR 17.00. This Information Security Program is effective as of March 1, 2010 (the "**Effective Date**").

2. Definitions

For purposes of this Information Security Program, the following definitions apply to the associated capitalized terms. Additional terms are defined in context elsewhere herein.

2.1. **Covered Employees**. The term "**Covered Employees**" means those GBCVB employees that have access to Relevant Records.

2.2. **Data Security Coordinator**. The term "**Data Security Coordinator**" has the meaning set out in Section 4.1.1 (Designation of Data Security Coordinator).

2.3. **Designated Personnel**. The term "**Designated Personnel**" has the meaning set out in Section **Error! Reference source not found.** (Designation of Personnel).

2.4. **Personal Information**. The term "**Personal Information**" means a Massachusetts resident's (i) first name and last name, or first initial and last name, in combination with (ii) any one or more of the following data elements that relate to a particular resident: (a)

Social Security number, (b) driver's license number or state-issued identification card number; or (c) financial account number, credit card number or debit card number. The term "Personal Information" expressly excludes information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

2.5. **Record**. The term "**Record**" means any material (including both electronic and paper) upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of the physical form or characteristics.

2.6. **Relevant Records**. The term "**Relevant Records**" has the meaning set out in Section 3**Error! Reference source not found.** (Scope).

2.7. **Third-Party Service Provider**. The term "**Third-Party Service Provider**" has the meaning set out in Section 5.3 (Third-Party Service Providers).

3. SCOPE

This Information Security Program, and the measures that have been implemented pursuant to it to protect GBCVB's employees, customers and members extends to all of GBCVB's Records that contain Personal Information about Massachusetts residents (collectively, the "**Relevant Records**").

4. DESIGNATIONS AND RESPONSIBILITIES

4.1 Data Security Coordinators

4.1.1 Designation of Data Security Coordinators. GBCVB's Senior Vice President has designated two employees with overall responsibility for the Information Security Program (each, a "**Data Security Coordinator**"). The Data Security Coordinators will continue to be responsible until the Senior Vice President of Administration determines otherwise. The current Data Security Coordinators are identified on Schedule 4.1.24.1 (Data Security Coordinators).

4.1.2 Responsibilities of Data Security Coordinators. In addition to the other responsibilities set out in this Information Security Program, the Data Security Coordinators are responsible for:

4.1.2.1 Generally overseeing the Information Security Program to ensure that it is properly implemented and functioning as intended;

4.1.2.2 Overseeing the efforts of all Designated Personnel;

4.1.2.3 Reviewing and approving all policies and procedures developed and implemented pursuant to this Information Security Program, as well as all revisions to the Information Security Program;

4.1.2.4 Ensuring that all Covered Employees are aware of any revisions to the Information Security Program and related policies and procedures;

4.1.2.5 Performing all compliance tasks set out in Section 9 (Compliance Efforts); and

4.2 Designated Personnel

4.2.1 Designation of Personnel. The Data Security Coordinators have assigned various personnel to certain tasks set out in this Information Security Program (collectively, the "**Designated Personnel**"). All assignments were made in order to assist the Data Security Coordinators in the development, implementation, monitoring and maintenance of the Information Security Program. A list of all Designated Personnel, their titles, and the tasks for which they are responsible, is included on Schedule0 (Designated Personnel).

4.2.2 Responsibilities of Designated Personnel. Designated Personnel are responsible for all tasks to which they are assigned including all related development, implementation, monitoring and maintenance efforts for each task. For example, if the Data Security Coordinators approve additional computer system monitoring measures, the Data Protection Coordinators must implement those new measures, monitor them to ensure that they are effective, and maintain them until the Data Security Coordinators instruct otherwise.

5. INFORMATION SECURITY PROGRAM IMPLEMENTATION

The Implementation Coordinators are responsible for the development and implementation tasks set out in this Section 5(Information Security Program Implementation).

5.1 Data Security Risk Assessment. The Data Security Coordinators and the Implementation Coordinators have identified and assessed both reasonably foreseeable internal and external risks to the security, confidentiality and integrity of all Relevant Records (the "**Data Security Risk Assessment**"). They will perform additional Data Security Risk Assessments (i) annually, and (ii) when any new internal or external risk is identified between each annual Data Security Risk Assessment.

5.1.1 Existing Security Measures. The Data Security Coordinators and Implementation Coordinators have evaluated the effectiveness of GBCVB's existing security measures designed to safeguard against the loss or theft of Relevant Records due to the internal and external risks identified in the Data Security Risk Assessment. In addition to other measures, GBCVB has scrutinized:

5.1.1.1 Covered Employee training including, but not limited to, temporary and contract employees (if any);

5.1.1.2 Covered Employee compliance with existing policies and procedures; and

5.1.1.3 The means implemented for detecting and preventing failures of the security measures put in place to protect all Relevant Records.

5.1.2 Improvement of Existing Measures. The Implementation Coordinators have improved, where necessary, those security measures that were determined to be ineffective.

5.2 Covered Employee Use and Transportation of Relevant Records Offsite. Covered Employees are restricted from keeping, accessing and transporting Relevant Records outside of GBCVB's premises. For example, Covered Employees shall not take Relevant Records from GBCVB's premises without first obtaining necessary permissions. A detailed list of the restrictions are set out on Schedule (Use and Transportation of Relevant Records Offsite).

5.3 Third-Party Service Providers. The term "**Third-Party Service Provider**" means any third party engaged by GBCVB to perform services related to GBCVB's activities, and that is given Relevant Records by GBCVB or has access to Relevant Records.

5.3.1 Third-Party Service Providers; Provider Protection. The Implementation Coordinators have taken reasonable steps (i) to verify that all existing Third-Party Service Providers are capable of maintaining appropriate security measures to protect Personal Information contained in Relevant Records consistent with Regulation 201 and any applicable federal regulations, and (ii) to select and retain only those future Third-Party Service Providers that are capable of maintaining appropriate security measures to protect Personal Information contained in Relevant Records consistent with Regulation 201 and any applicable federal regulations. **Such steps included, for example, verifying that a particular Third-Party Service Provider has implemented its own information security program, obtaining a copy of any such program, and providing it to outside legal counsel for review.**

5.3.2 Third-Party Service Provider Compliance. The Implementation Coordinators will review GBCVB's relationships with all Third-Party Service Providers both (i) annually, and (ii) as new agreements with Third-Party Service Providers are executed. The purpose of this review is to verify that all Third-Party Service Providers are meeting, at least, those requirements set out in Section 5.3.1 (Third-Party Service Providers; Provider Protection).

5.3.3 Third-Party Service Provider Agreement Provisions.

5.3.3.1 Post Effective Date Agreements. The Implementation Coordinators will ensure that those agreements between GBCVB and any Third-Party Service Provider that it engages after the Effective Date contain a provision requiring the Third-Party Service Provider to implement and maintain appropriate security measures to protect Personal Information contained in Relevant Records consistent with Regulation 201 and applicable federal regulations (each, a "**Compliance Provision**").

5.3.3.2 Pre-Existing Agreements. On or before March 1, 2012, the Implementation Coordinators shall, with respect to agreements GBCVB has with Third-Party Service Providers in effect prior to the Effective Date, either (i) amend such agreements by including a Compliance Provision, or (ii) develop and implement an alternative solution with applicable Third-Party Service Providers consistent with Regulation 201.

5.3.4 Third-Party Service Provider List. A list of all existing Third-Party Service Providers is included on Schedule0(the "**Third-Party Service Provider List**"). The Implementation Coordinators will revise the Third-Party Service Provider List as existing Third-Party Service Providers are removed and new ones added.

6. MONITOR AND REVIEW

The Oversight Coordinators are responsible for the tasks related to monitoring and reviewing the Information Security Program set out in this Section 6 (Monitor and Review).

6.1 Monitoring of the Information Security Program.

6.1.1 Monitor Reports. The Data Security Coordinators are regularly monitoring the Information Security Program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to, or use of, Relevant Records. Annually, the Data Security Coordinators will produce a Monitor Report.

6.1.2 Revisions to Information Security Program. After the Monitor Reports are completed, the Data Security Coordinators will meet and review the Monitor Reports. They will then work together to identify any revisions or upgrades to the Information Security Program that may be necessary to minimize the risk of access to, or use of, Relevant Records.

6.2 Scope Review of Security Measures. In addition to regularly monitoring the Information Security Program itself, the Data Security Coordinators will periodically review the scope and application of all security measures implemented to protect Relevant Records from unauthorized access or use (each, a "Security Review"). Security Reviews will be conducted (i) at least annually, and (ii) whenever there is a material change in GBCVB's business practices that may reasonably implicate the security or integrity of Relevant Records. Such material changes may include, for example, the collection of Personal Information through a new questionnaire, the conversion of paper records to electronic records, or the introduction of new computer networking capabilities.

7. TRAINING

The Data Security Coordinators are responsible for developing a training program (the "Training Program") to provide initial and ongoing training relating to the Information Security Program. Among other things, the goal of the Training Program is to stress the importance of protecting Personal Information.

7.1. Training Program. The Training Program includes: (i) an overview of the Information Security Program and its objectives, (ii) the policies and procedures that GBCVB has implemented to safeguard all Relevant Records, (iii) the Covered Employees' obligations under the Information Security Program including, but not limited to, what actions to take should they uncover a theft of Relevant Records; and (iv) instruction on the proper use of GBCVB's electronic security measures, including its computer system measures designed to protect Relevant Records. In addition, each Covered Employee will receive a copy of the Information Security Program, and must certify to such receipt in writing.

7.2. Updates to Training Program. The Data Security Coordinators will revise the Training Program as new policies and procedures relating to Relevant Records are developed and implemented.

7.3. Training of Existing Covered Employees. All existing Covered Employees must have completed the Training Program either before, or within a reasonable time after, the Effective Date.

7.4. Training of New Covered Employees. The Data Security Coordinators will ensure that all new Covered Employees have completed the Training Program within a reasonable time of the start date of their employment.

7.5. Annual Training. The Data Security Coordinators will provide an annual presentation of the Training Program. All Covered Employees must participate in the annual Training Program regardless of whether they have participated in a previous Training Program.

8. SECURITY

The Data Security Coordinators are responsible for the security measures set out in this Section 8(Security) relating to the security of Relevant Records.

8.1. Restrictions on Physical Access to Relevant Records. Reasonable physical restrictions on physical access to Relevant Records have been implemented. Specifically:

8.1.1. Access Restrictions. Physical access restrictions to Relevant Records have been implemented. Such restrictions include, for example, limiting access by securing applicable Relevant Records in locked containers, limiting the number of available keys to locked containers, and only allowing supervised access to the Relevant Records.

8.1.2. Secure Storage. All applicable Relevant Records must be stored in locked facilities, storage areas or containers. In addition, the Data Security Coordinators shall ensure that all relevant facilities, storage areas and containers are locked at the end of the

working day, and that Covered Employees using Relevant Records return them to their storage locations before leaving work for the day unless otherwise set out in Schedule 0 (Use and Transportation of Relevant Records Offsite).

8.2. Restrictions on Access to Electronic Records. To the extent technically feasible, GBCVB has implemented the following restriction measures to electronic access to Relevant Records:

8.2.1. Secure Access Control Measures

8.2.1.1. Access Restrictions. Access to electronic versions of Relevant Records are restricted to only those GBCVB employees who need access to such Relevant Records to perform their job responsibilities. Such restrictions include, for example, isolating all Relevant Records to a single storage location, which is only accessible by GBCVB employees with appropriate administrative privileges.

8.2.1.2. Identification and Passwords. Unique user accounts and passwords have been assigned to all current GBCVB employees with computer access, and will be assigned to new GBCVB employees with computer access. Such assignments have been reasonably designed to maintain the integrity and security of all implemented access controls. All assigned passwords are not vendor-supplied default passwords.

8.2.1.3. Password Resetting. User passwords will be reset at predetermined intervals and prohibitions against selecting previously- used passwords have been implemented.

8.2.2. Secure User Authentication Protocols. The following measures relating to secure user authentication protocols have been implemented:

8.2.2.1. Means to control user IDs and other identifiers;

8.2.2.2. Secure methods of assigning and selecting passwords;

8.2.2.3. Controls for data security passwords that ensure that Such passwords are kept in a location and/or format that does not compromise the security of the Relevant Records they protect;

8.2.2.4. Requiring re-login of a user should a computer remain inactive for an extended period of time;

8.2.2.5. Restricting access to Relevant Records to only active users and active user accounts; and

8.2.2.6. Blocking access to Relevant Records after multiple unsuccessful attempts to access them using a particular access method. For example, access to Relevant Records will be prohibited if an incorrect password associated with a particular

user account is provided five (5) consecutive times.

8.2.3. Software Protection Measures.

8.2.3.1. Firewall Protection. Firewall protection has been installed on all computers in GBCVB's control that (i) store or are able to access Relevant Records, and (ii) are capable of accessing the internet. The Data Protection Coordinators will also take all reasonable steps to ensure that the installed firewall protection is up-to-date, and will regularly update it as newer versions become available.

8.2.3.2. Operating System Security Patches. Operating system security patches that are reasonably designed to maintain the integrity of Personal Information have been installed on all computers in GBCVB's control that (i) store or are able to access Relevant Records, and (ii) are capable of accessing the internet. The Data Protection Coordinators will take reasonable steps to ensure that the versions of the operating system security patches are up-to-date, and will regularly update them as newer versions become available.

8.2.3.3. Security Agent Software. Security agent software has been installed on all computers in GBCVB's control (the "Security Agent Software"). The Security Agent Software contains: (i) malware protection, (ii) reasonably up-to-date patches; and (iii) reasonably up-to-date virus definitions. The Data Protection Coordinators will regularly review the Security Agent Software to verify that the versions of the malware protection, patches and virus definitions are up-to-date, and will install newer versions as they become available.

8.2.4. Encryption of Relevant Records. The term "Encrypt" or "Encryption" means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

8.2.4.1. Encryption of Stored Relevant Records. The Data Protection Coordinators have Encrypted all Relevant Records stored on laptops or other portable devices in GBCVB's control that are capable of storing, receiving or transmitting Relevant Records.

8.2.4.2. Encryption of Relevant Records During Transmission. The Data Protection Coordinators have, to the extent technically feasible, introduced Encryption processes for all Relevant Records that are transmitted by electronic means including wired networks, wireless networks, and other public networks.

8.2.5. Maintenance of Electronic Record Restriction Policy. The Data Security Coordinators are responsible for maintaining and updating the measures set out in this Section 8.2(Restrictions on Access to Electronic Records). Such efforts include, for example, annual reviews of the measures to ensure that all components are functioning as intended, and upgrading certain measures as new, more secure,

methods become available.

8.3. System Monitoring

8.3.1. System Monitoring Efforts. The Data Security Coordinators are responsible for reasonably monitoring all of the computer systems for unauthorized access to, or use of, Relevant Records. Monitoring unauthorized access and use may include, for example, attempts to access restricted files, flagging outgoing email that contains Relevant Records as attachments, and monitoring to determine if third parties have made efforts to "hack" into GBCVB's computer system.

8.3.2. System Monitoring; Reviewing and Updating. The Data Security Coordinators will perform audits, at least annually, of their system monitoring efforts to determine (i) their effectiveness, and (ii) those areas in which the efforts could be improved. After each audit, the Data Security Coordinators will revise the measures should they determine that they could be improved; provided, however that such improvements will not be incorporated if the Data Security Coordinators determine that such improvements would be unduly burdensome.

8.4. Exiting Employees

8.4.1. Removal of Access to Relevant Records. The Data Security Coordinators are responsible for the treatment of all exiting employees including, but not limited to, terminated employees, retiring employees, and employees that have voluntarily resigned from their employment at GBCVB (collectively, the "Exiting Employees"). The Data Security Coordinators will ensure that all Exiting Employees are prevented from having access to Relevant Records prior to their leaving the premises after being terminated. Access removal includes both physical and electronic access. Steps taken to ensure that access is removed include, at a minimum: (i) deactivating any applicable user accounts and passwords, (ii) confiscating any keys to file cabinets and other storage areas containing Relevant Records in the Exiting Employee's control, (iii) confiscating any keys or ID badges that would allow the Exiting Employee to access GBCVB's physical premises; and (iv) notifying building security that a particular Exiting Employee has been terminated.

8.4.2. Return of Relevant Records. The Data Security Coordinator will also collect from the Exiting Employee (i) all Relevant Records, in any form or medium, currently in the Exiting Employee's possession or control, and (ii) all copies of Relevant Records, in any form or medium, currently in the Exiting Employee's possession or control.

8.5. Restrictions on Visitor Access. The Data Security Coordinators have taken steps to ensure that visitors are prohibited from accessing GBCVB's premises without first passing through adequate security measures to verify their identity and determine whether a particular visitor has a legitimate purpose for entering GBCVB's premises. In addition, all visitors will be required to wear plainly visible "guest" badges, and will not be permitted access to any area of GBCVB's premises where Relevant Records are located.

9. COMPLIANCE EFFORTS

9.1. Incident Response

9.1.1. Security Breach; Responsive Actions. Upon any breach of the security measures implemented by GBCVB to protect Relevant Records, the Data Security Coordinators shall, as soon as practicable, review the breach and revise the Information Security Program and GBCVB's business practices to minimize the likelihood of a reoccurrence of the same, or a similar, breach.

9.1.2. Documentation of Responsive Actions. The Data Security Coordinators will document any incident involving a breach of the security measures implemented by GBCVB to protect Relevant Records (each, an "Incident Report"). Each Incident Report will include, at a minimum: (i) a post-incident review of the security breach itself, (ii) the responsive actions taken in connection with the security breach; and (iii) those revisions to the Information Security Program or GBCVB's business practices that were made to minimize the likelihood of a reoccurrence of the same, or a similar, breach.

9.2. Disciplinary Measures. The Senior Vice President of Administration will impose disciplinary measures on any GBCVB employee who violates the policies and procedures set out in this Information Security Program. The Data Security Coordinators, in consultation with GBCVB's Vice President of Administration will determine the particular disciplinary measure to be taken on an individual basis, based on the nature and severity of a particular infraction.

10. COVERED EMPLOYEE OBLIGATIONS

In addition to the other responsibilities set out in this Information Security Program, all Covered Employees shall be responsible for:

10.1. Regularly reviewing this Information Security Program, including all revisions and updates that are made to the Information Security Program and related policies and procedures;

10.2. Complying with all policies and procedures that have been developed and implemented as a result of this Information Security Program;

10.3. Understanding and complying with any responsibilities given to you pursuant to Section 4.2 (Designated Personnel) of this Information Security Program, including all related development, implementation, monitoring and maintenance obligations;

10.4. Knowing and complying with all policies and procedures related to the access, use and treatment of all Relevant Records as set out in Section 8 (Security);

10.5. Reviewing all internal and external risks identified in the Data Security Risk Assessment in order to be more aware of potential threats to the integrity and security of Relevant Records (Data Security Risk Assessment);

10.6. Feedback and suggestions to the Data Security Coordinators relating to the policies and procedures implemented to protect Relevant Records;

10.7. Reporting to the Data Security Coordinators all suspicious activity relating to Relevant Records such as unauthorized use and Transportation of Relevant Records by other employees, or unauthorized attempts to access Relevant Records by other parties;

10.8. Immediately reporting any discovered security breaches to the Data Security Coordinators;

10.9. Understanding and complying with all physical and electronic security measures adopted to protect the integrity and confidentiality of Relevant Records as set forth in Section 8 (Security);

10.10. Protecting all assigned passwords so that they are not accessible or used by other parties; and

10.11. Complying with all exit requirements set out in Section 8.4 (Exiting Employees).

SCHEDULE 4.1.24.1:
DATA SECURITY COORDINATORS

The Vice President of Operations and Human Resource Coordinator have been designated by GBCVB's Senior Vice President of Administration as the Data Security Coordinators. Chief of Staff for the Boston Convention and Exhibition Center (BCEC) has designated the CMC Executive Assistant as the Data Security Coordinator for BCEC.

SCHEDULE 4.2:
DESIGNATED PERSONNEL

Position Title	Section No.	Section Title	Name of Designated Personnel
Implementation Coordinator	5.1	Data Security Risk Assessment	Director of Finance, CMC Executive Assistant
	5.2	Covered Employee Use and Transportation of Relevant Records Offsite	Human Resource Coordinator
	5.3.1	Third-Party Service Providers	Human Resource Coordinator
Oversight Coordinator	6.1	Monitoring of the Information Security Program	VP of Operations, Human Resource Coordinator, CMC Executive Assistant
	6.2	Scope Review of Security Measures	VP of Operations, Human Resource Coordinator
Training Coordinator	7	Training	Human Resource Coordinator, VP of Operations
Data Protection Coordinators	8.1	Restrictions on Physical Access to Relevant Records	Human Resource Coordinator, CMC Executive Assistant
	8.2	Restrictions on Access to Electronic Records	VP of Operations
	8.3	System Monitoring	VP of Operations
	8.4	Exiting Employees	Human Resource Coordinator, VP of Operations, CMC Executive Assistant
	8.5	Restrictions on Visitor Access	Human Resource Coordinator, VP of Operations, CMC Executive Assistant

SCHEDULE 5.2
USE AND TRANSPORATION OF RELEVANT RECORDS OFFSITE

Employees of GBCVB may not keep, access or transport Relevant records outside of GBCVB's premises. Only an approved storage facility may transport and keep GBCVB's Relevant records.

SCHEDULE 5.3.4
THIRD-PARTY SERVICE PROVIDER LIST

No.	Third-Party Service Provider	Contact Representative	Contact Info.	Type of Relevant Records
	Blue Cross & Blue Shield of Massachusetts	Katie Cloutier	617-246-8829 KatherineCloutier@bcbsma.com	Employee name and Social Security number
	Lincoln Financial	Kathleen McKeon	617-587-5997 clientservice@lfg.com	Employee name and Social Security number
	ADP Payroll	Customer Service	855-669-6160	Employee name, Social Security number and for some employees, Personal Financial Account information
	Flexible Spending Account	The Benefits Center Aimee Guertin	860-351-0117 aguertin@myhcg.com	Employee Name, Social Security Number
	The Health Consultants Group, LLC	Keyne Reid	860-351-0103 kreid@myhcg.com	Employee name, Social Security Number
	Centinel Financial Group	John McAvoy	781-446-5008	Employee Name, Social Security Number, 401(k) Account information
	Group Benefit Strategies	Gretchen Grogan	508-832-0490 ggrogan@gbs-consult.com	Employee Name and Social Security Number
	Aflac	Liz Weiner	781-784-3899 Elizabeth_weiner@us_aflac.com	Employee Name and Social Security Number

THIRD-PARTY SERVICE PROVIDER LIST (CONTINUED)

No.	Third-Party Service Provider	Contact Representative	Contact Info.	Type of Relevant Records
	Safeguard Records Management	Customer Service	617-888-795-7233	Employee Name, Social Security Number and Personal Financial Account Numbers
	Bank of America	Customer Service	1-877-895-2613	Customer Name & Credit Card Number
	Citizens Bank	Matthew Appel	781-789-7551	Customer Name & Credit Card Number
	iCorps	Michael Lewis : mlewis@icorps.com 888-642-6484 Josh Weigner jweigner@icorps.com 617-410-6440	Help Desk 616-868-2000 help@icorps.com	Passwords