Black Gaming LLC **Information Security and Access Control Policy**	**Doc. Version:**	2.0	Page 1 of 3
	Revised by:	BG LLC IT	**Revision Date:** New
	Effective Date:	8-24-07	
	Approval:	Director of IT Support	
	Filename:	Information Security and Access Control Policy v 2.0	

1.0 Responsibility

All who access **BLACK GAMING, LLC** data are considered responsible to abide by this policy.

2.0 Purpose

The purpose of this policy is to establish the protection of **BLACK GAMING, LLC's** computerized information systems, data, and software. In addition, it establishes the mandatory requirements that all full- and part-time employees, contractors, vendors, consultants, temporary staff, other workers including personnel affiliated with third parties, and agents of and at **BLACK GAMING, LLC** that need access to information assets are uniquely identified and authenticated; and are granted only the level of access that is appropriate and sufficient to perform their assigned job functions.

3.0 Scope

This policy applies to all areas of **BLACK GAMING, LLC** and to all full- and part-time employees, contractors, vendors, consultants, temporary staff, other workers including personnel affiliated with third parties, and agents with a **BLACK GAMING, LLC** owned or vendor-owned computer or workstation used to connect to the **BLACK GAMING, LLC** network locally or remotely accessing any network or server equipment or server application owned and/or administered or operated by the Company.

4.0 Policy

4.1. Information Security

Information contained in the **BLACK GAMING, LLC** systems is the property of **BLACK GAMING, LLC** and represent official **BLACK GAMING, LLC** records. Users who accept access to this information, whether on-line or in datasets, also accept responsibility for adhering to certain principles in the use and protection of that information:

- Information systems within **BLACK GAMING, LLC** shall be used only for and contain only data necessary for fulfillment of **BLACK GAMING, LLC**'s mission.
- **BLACK GAMING, LLC** information shall be used solely for the legitimate business of **BLACK GAMING, LLC**.
- Due care shall be exercised to protect **BLACK GAMING, LLC** information and systems from unauthorized use, disclosure, alteration or destruction.
- **BLACK GAMING, LLC's** data, regardless of who collects or maintains it, shall be shared among those employees whose responsibilities require knowledge of such information.
- Applicable federal and state laws (i.e. the Privacy Act), and **BLACK GAMING, LLC** policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate **BLACK GAMING, LLC** procedures shall be followed in reporting any breach of security or compromise of safeguards (e.g. Help Desk Procedure).
- All network clients and Windows servers are equipped with anti virus. The server application is configured to automatically obtain updates from the Symantec site, and send the appropriate update to all clients. All Windows servers and the company owned personal computers are protected by Anti-virus software. Updates are automatically distributed by a dedicated anti virus server and are replicated to all the servers. If a client has not been updated in 10 days, a manual update is pushed to the client. If the client does not respond in 14 days Active Directory disables the computer account. If the client does not respond in 30 days the computer account is deleted.
- Email virus & spam filtering at the gateway is performed by a Barracuda Appliance.

- Information systems capabilities can be re-established within an acceptable time upon loss or damage by accident, malfunction, breach of security, or act of God.
- Users may not use, query, release or print information in any application which they have not been given deliberate access to, which can include, but is not limited to:
  - Personnel, leave, salary reports;
  - Mailing lists and labels; and
  - Private or public release of data to outside parties.

4.2. Access Control

Application security (i.e., user permissions and groups) will be designed and built such that users *only* have access to sensitive or confidential information as needed to perform their assigned job duties. User Accounts shall be managed, conform to IT procedures, and will reflect information security best practices as they apply to **BLACK GAMING, LLC.**

These IT procedures will reflect the following minimum baseline:

- **BLACK GAMING, LLC** uses the standard security principle of least privileged access and authorization such that users are only authorized the level of access to information assets that is necessary and required to perform their specific job responsibilities.
- User accounts are added, modified, and deleted ONLY upon completion of the System Access Request form in accordance with **BLACK GAMING, LLC's** approved account management standards and operational department procedures.
- Each account must have a unique identifier (User ID) and should conform to any/all established **BLACK GAMING, LLC** naming convention(s).
- Each user ID or account must be assigned a password (or appropriate and approved authentication method) that complies with the approved **BLACK GAMING, LLC** password standards. Initial passwords are assigned by the IT Department. User's initial logon using the assigned password will force a new password change prior to authentication. Periodic password changes are made by the password owner. See the Acceptable Use Policy; Password Policy section.
- All Temporary User accounts used for testing, contractors and temporary employees must have an account expiration date that coincides with the anticipated end of testing, contract or temporary employment. Temporary and contractor accounts will only be granted for 90 days, regardless of the anticipated employment length. The hiring manager must contact IT at the end of each 90 day period to renew the access. Each Temporary User account must have a clear description of its intended purpose documented in the account's in the appropriate comment section.
- Unused, dormant, or inactive accounts must be disabled and deleted in accordance to any/all approved **BLACK GAMING, LLC** IT Procedures.
- Information Technology is responsible for changing all system and application default passwords prior to placing in the **BLACK GAMING, LLC** operating environment and/or connecting to a live (non-test) **BLACK GAMING, LLC** network.
- User IDs/accounts must not be shared or used by anyone other than the User to whom the User ID is assigned; each account shall be assigned to a single person. Users shall be accountable for all activity associated with their assigned account.

4.3. Employee Responsibilities

Safeguarding of **BLACK GAMING, LLC** information systems and data shall be the responsibility of each employee with knowledge of the system or data. Specific responsibilities are as follows:

- **Management** - all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff and staff of other departments accessing their responsible system, according to their job functions, prior to submitting a System Access Request form for the provision of access. Managers of **BLACK GAMING, LLC** may appoint an individual within their staff to ensure these responsibilities are observed.
- **Users** - are responsible for the protection, privacy, and control of all information, regardless of the storage medium. Users must ensure that the information, stored in both soft copy and hard copy, is maintained and/or disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the information to which they have access, and may use this information only to support the normal functions of their administrative duties.
- **Information Technology** - is responsible for providing administrative & technical support in the area of information security for all users. This support includes, but is not limited to:

    - Creation, modification, and deletion of user IDs, after appropriate approval has been obtained.
    - Providing access to administrative systems, transactions, or production after appropriate approval.
    - Information Technology is responsible for changing all system and application default passwords prior to placing in the **BLACK GAMING, LLC** operating environment and/or connecting to a live (non-test) **BLACK GAMING, LLC** network.

4.4. Employee Termination

Access to **BLACK GAMING, LLC's** information shall be immediately disabled for terminated employees upon formal notification to the IT Department. Under no circumstances shall access be granted to a terminated employee. It is the responsibility of the manager of the terminated employee and/or HR to communicate termination status to the IT Department and any other pertinent groups.

5.0 Enforcement

Management will determine appropriate use and enforce this policy. A violation of this policy will be acted upon immediately, and appropriate corrective action taken. Any violation of this Policy by the employee may result in disciplinary action, to and including, the following:

- Offenses will be reported to the employee's manager for review
- Probation
- Termination of employment
- Other disciplinary action
- Civil and/or criminal prosecution

6.0 Additional Information

Any inquiries relating to this Information Security and Access Control Policy should be directed to the Director of IT Support.

Black Gaming LLC **Information Security and Access Control Policy**	**Doc. Version:**	2.0	Page 1 of 3
	Revised by:	BG LLC IT	**Revision Date:** New
	Effective Date:	8-24-07	
	Approval:	Director of IT Support	
	Filename:	Information Security and Access Control Policy v 2.0	

1.0 Responsibility

All who access **BLACK GAMING, LLC** data are considered responsible to abide by this policy.

2.0 Purpose

The purpose of this policy is to establish the protection of **BLACK GAMING, LLC's** computerized information systems, data, and software. In addition, it establishes the mandatory requirements that all full- and part-time employees, contractors, vendors, consultants, temporary staff, other workers including personnel affiliated with third parties, and agents of and at **BLACK GAMING, LLC** that need access to information assets are uniquely identified and authenticated; and are granted only the level of access that is appropriate and sufficient to perform their assigned job functions.

3.0 Scope

This policy applies to all areas of **BLACK GAMING, LLC** and to all full- and part-time employees, contractors, vendors, consultants, temporary staff, other workers including personnel affiliated with third parties, and agents with a **BLACK GAMING, LLC** owned or vendor-owned computer or workstation used to connect to the **BLACK GAMING, LLC** network locally or remotely accessing any network or server equipment or server application owned and/or administered or operated by the Company.

4.0 Policy

4.1. Information Security

Information contained in the **BLACK GAMING, LLC** systems is the property of **BLACK GAMING, LLC** and represent official **BLACK GAMING, LLC** records. Users who accept access to this information, whether on-line or in datasets, also accept responsibility for adhering to certain principles in the use and protection of that information:

- Information systems within **BLACK GAMING, LLC** shall be used only for and contain only data necessary for fulfillment of **BLACK GAMING, LLC**'s mission.
- **BLACK GAMING, LLC** information shall be used solely for the legitimate business of **BLACK GAMING, LLC**.
- Due care shall be exercised to protect **BLACK GAMING, LLC** information and systems from unauthorized use, disclosure, alteration or destruction.
- **BLACK GAMING, LLC's** data, regardless of who collects or maintains it, shall be shared among those employees whose responsibilities require knowledge of such information.
- Applicable federal and state laws (i.e. the Privacy Act), and **BLACK GAMING, LLC** policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate **BLACK GAMING, LLC** procedures shall be followed in reporting any breach of security or compromise of safeguards (e.g. Help Desk Procedure).
- All network clients and Windows servers are equipped with anti virus. The server application is configured to automatically obtain updates from the Symantec site, and send the appropriate update to all clients. All Windows servers and the company owned personal computers are protected by Anti-virus software. Updates are automatically distributed by a dedicated anti virus server and are replicated to all the servers. If a client has not been updated in 10 days, a manual update is pushed to the client. If the client does not respond in 14 days Active Directory disables the computer account. If the client does not respond in 30 days the computer account is deleted.
- Email virus & spam filtering at the gateway is performed by a Barracuda Appliance.

- Information systems capabilities can be re-established within an acceptable time upon loss or damage by accident, malfunction, breach of security, or act of God.
- Users may not use, query, release or print information in any application which they have not been given deliberate access to, which can include, but is not limited to:
  - Personnel, leave, salary reports;
  - Mailing lists and labels; and
  - Private or public release of data to outside parties.

4.2. Access Control

Application security (i.e., user permissions and groups) will be designed and built such that users *only* have access to sensitive or confidential information as needed to perform their assigned job duties. User Accounts shall be managed, conform to IT procedures, and will reflect information security best practices as they apply to **BLACK GAMING, LLC.**

These IT procedures will reflect the following minimum baseline:

- **BLACK GAMING, LLC** uses the standard security principle of least privileged access and authorization such that users are only authorized the level of access to information assets that is necessary and required to perform their specific job responsibilities.
- User accounts are added, modified, and deleted ONLY upon completion of the System Access Request form in accordance with **BLACK GAMING, LLC's** approved account management standards and operational department procedures.
- Each account must have a unique identifier (User ID) and should conform to any/all established **BLACK GAMING, LLC** naming convention(s).
- Each user ID or account must be assigned a password (or appropriate and approved authentication method) that complies with the approved **BLACK GAMING, LLC** password standards. Initial passwords are assigned by the IT Department. User's initial logon using the assigned password will force a new password change prior to authentication. Periodic password changes are made by the password owner. See the Acceptable Use Policy; Password Policy section.
- All Temporary User accounts used for testing, contractors and temporary employees must have an account expiration date that coincides with the anticipated end of testing, contract or temporary employment. Temporary and contractor accounts will only be granted for 90 days, regardless of the anticipated employment length. The hiring manager must contact IT at the end of each 90 day period to renew the access. Each Temporary User account must have a clear description of its intended purpose documented in the account's in the appropriate comment section.
- Unused, dormant, or inactive accounts must be disabled and deleted in accordance to any/all approved **BLACK GAMING, LLC** IT Procedures.
- Information Technology is responsible for changing all system and application default passwords prior to placing in the **BLACK GAMING, LLC** operating environment and/or connecting to a live (non-test) **BLACK GAMING, LLC** network.
- User IDs/accounts must not be shared or used by anyone other than the User to whom the User ID is assigned; each account shall be assigned to a single person. Users shall be accountable for all activity associated with their assigned account.

4.3. Employee Responsibilities

Safeguarding of **BLACK GAMING, LLC** information systems and data shall be the responsibility of each employee with knowledge of the system or data. Specific responsibilities are as follows:

- **Management** - all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff and staff of other departments accessing their responsible system, according to their job functions, prior to submitting a System Access Request form for the provision of access. Managers of **BLACK GAMING, LLC** may appoint an individual within their staff to ensure these responsibilities are observed.
- **Users** - are responsible for the protection, privacy, and control of all information, regardless of the storage medium. Users must ensure that the information, stored in both soft copy and hard copy, is maintained and/or disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the information to which they have access, and may use this information only to support the normal functions of their administrative duties.
- **Information Technology** - is responsible for providing administrative & technical support in the area of information security for all users. This support includes, but is not limited to:

    - Creation, modification, and deletion of user IDs, after appropriate approval has been obtained.
    - Providing access to administrative systems, transactions, or production after appropriate approval.
    - Information Technology is responsible for changing all system and application default passwords prior to placing in the **BLACK GAMING, LLC** operating environment and/or connecting to a live (non-test) **BLACK GAMING, LLC** network.

4.4. Employee Termination

Access to **BLACK GAMING, LLC's** information shall be immediately disabled for terminated employees upon formal notification to the IT Department. Under no circumstances shall access be granted to a terminated employee. It is the responsibility of the manager of the terminated employee and/or HR to communicate termination status to the IT Department and any other pertinent groups.

5.0 Enforcement

Management will determine appropriate use and enforce this policy. A violation of this policy will be acted upon immediately, and appropriate corrective action taken. Any violation of this Policy by the employee may result in disciplinary action, to and including, the following:

- Offenses will be reported to the employee's manager for review
- Probation
- Termination of employment
- Other disciplinary action
- Civil and/or criminal prosecution

6.0 Additional Information

Any inquiries relating to this Information Security and Access Control Policy should be directed to the Director of IT Support.