NEVADA STATE BOARD OF MASSAGE THERAPY
POLICY AND PROCEDURE

Subject: Board Owned Computers and Information Technology Systems	Policy No. 4.2.1	
	Issued By: Board	Distribution: Nevada State Board of Massage Therapy Members and Employees
	Amends/Supersedes	
Reference(s): Provisions of NRS 242.300 and NAC governing conduct and public employees. State Consolidated Policy 3.4.1		Effective Date: 11/20/2019 Updated: 01/10/2024

I. PURPOSE

The purpose of this agreement is to ensure all Nevada State Board of Massage Therapy (NSBMT) employees, contractors, partners, and any other individuals that have access to state Information Technology (IT) resources understand NSBMT policies related to the access and use of those resources.

II. POLICY

IT resources within NSBMT are to be used in a manner that supports the mission of NSBMT. IT resources refer to all equipment, hardware, software or networks (including wireless networks) and includes computers, e-mail applications and state internet and intranet access (including when accessed through personally owned computers). The systems range from multi-user systems to single-user terminals and personal computers, whether free-standing or connected to networks.

In addition, all users are required to adhere to relevant Office of the Chief Information Officer (OCIO) and State Policy, Standards & Procedures (PSPs) as outlined within the scope of each standard/procedure. All EITS and State PSPs can be viewed at: https://it.nv.gov/Governance/Security/State_Security_Policies_Standards___Procedures/.

III. SCOPE

This acceptable use agreement governs the use of computers, networks, and other IT resources at the NSBMT. This statement applies to all NSBMT employees and contractors, and all other persons who may legally or illegally use or attempt to use computer resources owned or managed by the agency, and/or are connected by any means to the state SilverNet Network. As a user of these resources, employees are responsible for reading and understanding this agreement.

IV. RESPONSIBILITY

A. Employees are responsible for complying with the requirements of this policy

B. Supervisors are responsible for:
   1. Informing current incumbent employees periodically of the content and intent of this policy.
   2. Taking disciplinary action when an employee is in violation of this policy.

C. The Executive Director shall be responsible for:
   1. Providing assistance to supervisors and employees in the interpretation and explanation of this policy.
   2. Assisting management in determining action to be taken if an employee violates this policy.

V. PROCEDURES

A. System Access:
   1. All users must safeguard the confidentiality, integrity, and availability of NSBMT systems, including password login, access codes, network access information and log-on IDs from improper access, alteration, destruction, or disclosure.
   2. Users shall only access or use NSBMT systems when authorized. Users must abide by NSBMT, OCIO and other State policies regarding the protection of data and information stored on these systems.
   3. Whenever a user ceases to be an employee, contractor, or other authorized user of NSBMT computer systems, such user shall not use NSBMT facilities, accounts, access codes, privileges, or information for which he/she is no longer authorized. This includes the return of all NSBMT IT resources including hardware, software, data, and peripherals.

B. Use of State Systems:
   1. Users must not use NSBMT systems to engage in activities that are unlawful or violate federal or state laws, NSBMT, State or OCIO security policies or in ways that would:
      a. Be disruptive, cause offense to others, or harm morale
      b. Be considered harassing or discriminatory, or create a hostile work environment
      c. Result in State or NSBMT liability, embarrassment, or loss of reputation
   2. Users must maintain the integrity of information and data stored on NSBMT systems by:
      a. Only introducing data that serves a legitimate business purpose
      b. Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization
      c. Protecting data and information stored on or communicated across NSBMT systems, and accessing appropriate data or information only when authorized

d. Protecting data and information communicated over internal or public networks to avoid compromising or disclosing nonpublic information or communications

3. While NSBMT systems are primarily intended for business purposes, limited (incidental and occasional) personal use may be permissible when authorized by management in writing and it does not:
   a. Interfere with work responsibilities or business operations
   b. Involve interests in personal outside business or other non-authorized organizations or activities (which may include, but are not limited to, selling personal property, soliciting for or promoting commercial ventures, or soliciting for or promoting charitable, religious, or political activities or causes)
   c. Violate any of the federal or state laws or NSBMT, State or OCIO security policies
   d. Lead to inappropriate cost to NSBMT functional units
   e. Non-work-related surfing and utilizing streaming services such as listening to music or watching videos is prohibited
   f. External Internet based instant messaging is prohibited
   g. Peer-to-peer file sharing is prohibited
   h. Checking of personal email is prohibited
   i. Users must check all electronic media, such as software, diskettes, CDs, and files for viruses when acquired through public networks (e.g., internet sites) or from outside parties by using virus detection programs prior to installation or use. If users suspect a virus, the applicable system(s) or equipment must not be used until the virus is removed. The matter must be immediately reported to the department's IT staff, applicable manager and/or supervisor.

C. Authorized Software:

Only NSBMT approved and properly licensed software will be used or installed on NSBMT computers and will be used according to the applicable software license agreements. All software must be approved by the Executive Director including shareware or other software that is easily downloadable from the internet.

D. Protecting Sensitive Data/Information:

1. Users must ensure that any nonpublic information, data or software that is stored, copied, or otherwise used on State systems is treated according to the State and NSBMT standards regarding nonpublic information and applicable agreements and intellectual property restrictions.
2. If users take "mobile" storage devices/media off State premises they need to take proper measures to ensure sensitive data is protected in the event that the devices/media are lost, stolen, or hacked. Mobile storage devices/media can include, but not limited to: laptops, thumb drives (USB flash drives), CDs and diskettes. If "personal information" or highly sensitive information is stored (e.g. names, addresses, SSNs, etc.) on these devices/media then it must be encrypted. In addition, users must obtain approval from their agency's management staff before taking sensitive information off state premises.

E. Email:

1. The State e-mail system is to be used to support NSBMT business by facilitating communication and transmission of documents and files between parties.
   a. Inappropriate use of e-mail includes, but is not limited to, sending and forwarding:
      i. Messages, including jokes or language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive, or otherwise inappropriate (for example, messages about age, race, gender, disability, sexual orientation, national origin or similar matters).
      ii. Pornographic or sexually explicit materials.
      iii. Chain letters.
      iv. Information related to religious materials, activities, or causes.
      v. Charitable solicitations unless sanctioned by the State or NSBMT Executive Director.
      vi. Auction-related information or materials unless sanctioned by the State or NSBMT Executive Director.
      vii. Software or copyrighted materials without a legitimate business or instructional purpose.
      viii. Large personal files containing graphics or audio files (such as photographs and music).
      ix. Materials related to personal commercial ventures or solicitations for personal gain.
      x. Information related to political materials, activities, or causes unless sanctioned or permitted by the State or NSBMT Executive Director.
      xi. Unauthorized or inappropriate mass distribution or communication.
      xii. Any other materials that would be improper under this policy or other State or NSBMT or OCIO policy.

F. Internet:

1. Use of the internet should be restricted to activities required to support NSBMT business.
2. Inappropriate use of the internet includes, but is not limited to, accessing, sending, or forwarding information about, or downloading from:
   a. Sexually explicit, harassing, or pornographic sites.
   a. "Hate sites" or sites that can be considered offensive or insensitive.
   b. Auction or gambling sites.
   c. Games, shareware, software, audio, video, or other materials that NSBMT is not licensed or legally permitted to use or transmit, or that are inappropriate or not required by State or NSBMT business.
   d. Offensive or insensitive materials, such as sexually or racially oriented topics.
   e. Any other materials that would be improper under other State or EITS policies.
   f. Intentional importation of viruses, key loggers, Trojans, or any other software that could be classified as malware or spyware.

G. Use of Personally Owned Systems for NSBMT Business:
   1. When personally owned systems are used for NSBMT business, NSBMT retains the right to any NSBMT records or materials developed for NSBMT use. Also, any materials must be appropriately safeguarded according to applicable standards including, but not limited to, virus protection, protected access and backups.
   2. When accessing state IT resources using personal systems, for example accessing SilverNet remotely from home (or other remote location) using a Virtual Private Network (VPN), users must take appropriate precautions to ensure that they do not introduce any viruses, spyware or malware to the state's networks or systems. Users must also ensure non-authorized individuals do not gain access to State resources using their personally owned system(s).

H. Use of Board-Owned Mobile Computing Devices:
   1. The rules described above in section 2 (Use of State Systems) also applies to Board owned mobile devices, such as smart phones and tablets issued to employees. Employees are to use the devices only for state business and are to exercise reasonable due diligence in securing the devices from loss or theft and to protect the device from software viruses and malware.
   2. Users can only install applications on Board owned mobile devices that have been approved by the Department IT Manager or the Department Information Security Officer.

I. Acceptable Use Agreement:
   1. The purpose of this agreement is to ensure all NSBMT employees, contractors, partners, and any other individuals that have access to state IT resources understand NSBMT policies related to the access and use of those resources.
   2. This acceptable use agreement governs the use of computers, networks, and other IT resources of NSBMT. This statement applies to all NSBMT employees and contractors, and all other persons who may legally or illegally use or attempt to use computer resources owned or managed by the department, and/or is connected by any means to the state SilverNet Network. As a user of these resources, you are responsible for reading and understanding this agreement.
   3. IT resources within NSBMT are to be used in a manner that supports the mission of NSBMT. IT resources refer to all equipment, hardware, software or networks (including wireless networks) and includes computers, e-mail applications and state internet and intranet access (including when accessed through personally owned computers). The systems range from multi-user systems to single-user terminals and personal computers, whether free-standing or connected to networks.
   4. In addition, all users are required to adhere to relevant Office of the Chief Information Officer (OCIO) and State Policy, Standards & Procedures (PSPs) as outlined within the scope of each standard/procedure. All OCIO and State PSPs can be viewed at: https://it.nv.gov/Governance/Security/State_Security_Policies_Standards___Procedures/.

J. Consequences:

Any inappropriate use of NSBMT computer systems or information may be grounds for discipline up to and including dismissal. Should disciplinary action be required, NSBMT progressive disciplinary procedures Policy No. 3.1.1 will be followed.

VI. POLICY EXCEPTION

On occasion there are special circumstances that may require an exception to this policy be granted. Exceptions, while not common, require the approval of the Executive Director.

VII. POLICY COMMUNICATION

All supervisors and managers of the NSBMT will provide their employees with a copy of this policy. Employees needing clarification should contact the Executive Director for assistance.

This policy is not a substitute for relevant law or regulation nor does it establish additional rights beyond those provided in law and regulation. This policy is intended to be used in conjunction with federal regulations, and State law.

ACCEPTABLE USE AGREEMENT

The purpose of this agreement is to ensure all Nevada Board of Massage Therapy (NSBMT) employees, contractors, partners, and any other individuals that have access to state Information Technology (IT) resources understand NSBMT's policies related to the access and use of those resources.

This acceptable use agreement governs the use of computers, networks, and other IT resources at the NSBMT. This statement applies to all NSBMT employees and contractors, and all other persons who may legally or illegally use or attempt to use computer resources owned or managed by the department, and/or is connected by any means to the state SilverNet Network. As a user of these resources, you are responsible for reading and understanding this agreement.

IT resources within NSBMT are to be used in a manner that supports the mission of NSBMT. IT resources refer to all equipment, hardware, software or networks (including wireless networks) and includes computers, e-mail applications and state internet and intranet access (including when accessed through personally owned computers). The systems range from multi-user systems to single-user terminals and personal computers, whether free-standing or connected to networks.

In addition, all users are required to adhere to relevant Office of the Chief Information Officer (OCIO) and State Policy, Standards & Procedures (PSPs) as outlined within the scope of each standard/procedure. All EITS and State PSPs can be viewed at: https://it.nv.gov/Governance/Security/State_Security_Policies_Standards___Procedures/.
.

CONSEQUENCES

Any inappropriate use of NSBMT computer systems or information may be grounds for discipline up to and including dismissal. Should disciplinary action be required, NSBMT progressive disciplinary procedures will be followed.

_____ _____

Employee Name (Please Print) Date

_____

Employee Signature

_____ _____

Supervisor Signature Date