Data Security Policy Approved at the March 12, 2019, NHRS Board meeting.

I. Purpose and Intent

This Policy governs all aspects of the handling (*e.g.*, creation, receipt, acquisition, storage, maintenance, access, use, disclosure, transmission, transportation, disposal, and destruction) of Protected Information that belongs to New Hampshire Retirement System ("NHRS") or that is within NHRS' possession, custody, or control. This Policy applies to all NHRS Employees, Trustees, Independent Investment Committee (IIC) members, and all other Persons who have access to or possession, custody, or control of Protected Information covered by this Policy. Only the Executive Director or the Director of IT may authorize a deviation from this Policy, to the extent any such deviation is deemed necessary or appropriate and permitted by Applicable Law.

The Protected Information covered by this Policy consists of Protected Health Information, Protected Personal Information, and Confidential Information. Protected Health Information and Protected Personal Information are specifically defined in the Definitions section of this Policy, and include a person's name or other identifying information in combination with that person's medical information, social security number, governmental identification number, or financial account number. Confidential Information is defined in the Definitions section, and includes any information that belongs to NHRS or that is within NHRS' possession, custody, or control and that is not generally known to the public or generally available from public sources.

II. Policy

A. Definitions

The following definitions apply to this Policy. If a term used in this Policy is not specifically defined here, the definitions in Applicable Law may be used to interpret this Policy.

NHRS: "NHRS" means New Hampshire Retirement System, but not a Data Contractor, independent contractor, or vendor of NHRS.

Applicable Law: "Applicable Law" means (a) New Hampshire Revised Statutes Annotated, including, but not limited to, Chapter 359-C, Section 19 to 21, and (b) all other local, state and federal laws and regulations applicable to Protected Information that belongs to NHRS or that is within NHRS' possession, custody, or control.

Biometric Identifier: "Biometric Identifier" means any method by which a Person can be uniquely identified using one or more distinguishing biological traits, including fingerprint, hand geometry, earlobe geometry, retina and iris patterns, and voice waves.

Confidential Information: "Confidential Information" means all information, documents, data, and other materials that belong to NHRS or that are within NHRS' possession, custody, or control that are not generally known to the public or generally available from public sources. This term includes, but is not limited to, the following: (1) information, documents, data, and other materials related to actual and prospective members and beneficiaries of NHRS; (2) information, documents, data, and other materials related to products and services of NHRS,

developments of NHRS, personnel and Employees, operations, administration, finance, agreements, costs, business plans, financial statements, tax returns, purchase orders, invoices, account information, and billing records; (3) information, documents, data, and other materials that are marked or designated with a word or symbol indicating that the document or information should be considered confidential, including “Confidential”, “Personal” or “Privileged”; and (4) information, documents, data, and other materials that NHRS informs the Employee are confidential or that the Employee knows or should know are confidential.

Data Contractor: “Data Contractor” means any Person, not an Employee, who performs or assists in performing a function or activity for or on behalf of NHRS involving the handling of Protected Information.

Data Incident: “Data Incident” or “Incident” means the handling of Protected Information without authorization, beyond the scope of authorization, or in a manner or to an extent that compromises Protected Information or violates Applicable Law. An Incident does not include the handling of Protected Information that is Encrypted. An Incident also does not include (a) the unintended or good faith handling of Protected Information by an Employee or Data Contractor related to fulfilling their duties for NHRS; or (b) the disclosure of Protected Information by an Employee or Data Contractor to another Employee or Data Contractor, as long as the Protected Information is not otherwise further handled without authorization, beyond the scope of authorization, or in a manner or to an extent that compromises the Protected Information or violates Applicable Law.

Electronic Device: “Electronic Device” means any digital, analog, or electronic machine, device, system, account or service used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data, including servers, routers, networks, hubs, desktop computers, laptops, tablets, handheld computers, smartphones, cellphones, electronic readers, music players, internal and external drives, USB drives, digital cameras and video recorders, photo and video storage media, compact discs, digital video discs, other data storage media, digital telephone and voicemail systems, photocopiers, calculators, cloud storage, social media, micro-blogs, and blogs.

Employee: “Employee” means a Person employed by NHRS, but not a Data Contractor, independent contractor, or vendor of NHRS.

Encrypt: “Encrypt” means to transform data through use of an algorithmic process into a form in which there is a low probability of assigning meaning to the data without the use of a confidential process, key, security code, access code, or password.

External Drive: “External Drive” means a digital, analog, or electronic machine or device external to a computer used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data, including hard drives, USB drives, photo and video storage media, compact discs, and digital video discs.

Information Systems: “Information Systems” means a system of multiple Electronic Devices used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data.

Laptop: “Laptop” means a computer designed to be transported from place-to-place by the user or that the user routinely transports from place-to-place, other than Tablets, Smartphones, or External Drives.

Person: “Person” means any individual or entity, including a sole proprietorship, partnership, corporation, limited liability company, limited liability partnership, professional association, professional corporation, S corporation, and any other entity whatsoever.

Policy: “Policy” means this Data Security Policy, as well as all predecessors, successors, additions, modifications, amendments, addenda, and appendices to this Policy.

Protected Health Information: “Protected Health Information” means (a) any information related to any physical or mental health or condition of an individual, the provision of health care to the individual, or the payment for health care for an individual, where (b) that information specifically identifies the individual, or there is a reasonable basis to believe that the information can be used to identify the individual.

Protected Information: “Protected Information” means Protected Health Information, Protected Personal Information, Confidential Information, and any other information that NHRS or the Security Officers designate as Protected Information.

Protected Personal Information: “Protected Personal Information” means (a) the last name of an individual, together with that individual’s first name or the first initial of the first name, in combination with any of the following for that individual (i) social security number, (ii) governmental identification number, including driver’s license and non-drivers identification number, (iii) credit, debit, insurance, or other financial account number, with or without any username, password, personal identification number, or other code necessary to access or control such account, and (iv) password, personal identification number, or other code used to access or control any credit, debit, insurance, or other financial account. This term does not include any information that is generally publically available, including from any local, state, or federal governmental records, as long as such information did not become generally publically available through the violation of a Person’s obligation to maintain the confidentiality of that information, including pursuant to this Policy, Applicable Law, or an applicable contract.

Smartphone: “Smartphone” means a handheld digital, analog, or electronic device used to create, receive, acquire, store, maintain, access, use, transmit, transport, analyze, or manipulate computerized or electronic data, including iPhones, Droid phones, Blackberries and other cellphones, other than Laptops, External Drives, or Tablets.

Strong Password: “Strong Password” means at least 12 characters consisting of a combination of at least one upper case, one lower case letter, one number, and one symbol.

Tablet: “Tablet” means a portable digital, analog, or electronic device used to create, receive, acquire, store, maintain, access, use, transmit, transport, analyze, or manipulate computerized or electronic data, including iPads, Droid tablets, and electronic readers, other than Laptops, External Drives, or Smartphones.

B. <u>Responsibilities of Employees</u>

1. *Handling of Protected Information*: Employees, Trustees, and IIC members should handle Protected Information only if and to the extent doing so is necessary or appropriate to perform their duties for NHRS and is permitted by this Policy. In doing so, Employees should handle only the minimum amount of Protected Information necessary or appropriate to perform those duties and will not permit any Person to handle Protected Information if that Person is not authorized to do so.

2. *Disclosure of Protected Information*: Employees should disclose Protected Information only to the following Persons and only under the following circumstances: (a) other Employees and Data Contractors if necessary or appropriate for them to perform their duties for NHRS; and (b) the Person about whom the Protected Information pertains and any other Person who that Person authorizes (in writing) NHRS to disclose such Protected Information to, but only Protected Information about that Person. The Director of IT may disclose, and authorize the disclosure of Protected Information, to other Persons to the extent such disclosure is necessary or appropriate and permitted by Applicable Law.

3. *Awareness and Training*: Employees should (a) acquire and maintain an awareness about the types of Protected Information at NHRS, the types of Protected Information they are authorized to handle, and their authority and responsibility with respect to it, and (b) participate in training provided by NHRS to safeguard Protected Information.

4. *Use of Information Systems*: Employees should handle Protected Information only using Information Systems and Electronic Devices covered by this Policy. Employees should not handle Protected Information using any personal Electronic Device (unless specifically covered by and operated pursuant to this Policy), or any personal account (including any email, webmail, social media, or cloud storage account), unless approved in writing by the Executive Director or Director of IT.

5. *Transmission of Protected Information*: Employees should transmit Protected Information externally by email, file transfer protocol, or other means of digital, analog, or electronic transmission only if (a) the entire transmission or the Protected Information transmitted is Encrypted and (b) the transmission complies with paragraph II, B.2.

6. *Transportation of Protected Information:* Employees should transport Protected Information only (a) if in electronic format, the Electronic Device used for the transportation, or the Protected Information being transported, is Encrypted and (b) if in hard copy format, the Protected Information is transported in a container that provides a level of security that is appropriate to the nature and scope of the Protected Information being transported and the other circumstances of the transportation of the Protected Information.

7. *Storage of Protected Information*: Employees should store Protected Information in electronic format only on Information Systems and Electronic Devices covered by this Policy. To the extent available and feasible, Employees should store Protected Information in electronic format only on the server or other Information Systems and only in the electronic filing location designated and/or appropriate for such Protected Information. Employees should store Protected Information in hard copy format only in a filing cabinet, filing room, or similar room at NHRS' facility that is locked or otherwise secured during non-working hours. If an Employee receives Protected Information in electronic format on an Electronic Device, and the Electronic Device or the Protected Information on it are not Encrypted, either (a) the Electronic Device

should be stored in a filing cabinet, filing room, or similar room that is locked or otherwise secured during non-working hours, or (b) the Protected Information should be transferred to an Electronic Device that it Encrypted and the original unencrypted Electronic Device will be returned to the Person from whom NHRS received it or destroyed in compliance with this Policy.

8. *Printing of Protected Information*: Employees should print or otherwise generate Protected Information in hard copy format only to the extent doing so is necessary or appropriate to perform their duties for NHRS, and the hard copy information generated is stored, maintained, disposed of, destroyed, and otherwise handled in accordance with this Policy.

9. *Laptops*: Employees should handle Protected Information on a Laptop only if (a) a Strong Password is required to access the Laptop and, (b) the entire Laptop, or the Protected Information on it, is Encrypted, and (c) the Laptop is owned by NHRS.

10. *Tablets and Smartphones*: Employees should handle Protected Information on a Tablet or Smartphone, including a personal Tablet or Smartphone, only if (a) a Strong Password or Biometric Identifier is required to access the Tablet or Smartphone or the Protected Information on it, and (b) the entire Tablet or Smartphone, or the Protected Information on it, is Encrypted. NHRS will implement controls in order to ensure that any Employee who accesses a NHRS email account using a Tablet or Smartphone, including a personal Tablet or Smartphone, is required to use a Strong Password or Biometric Identifier to access the Tablet or Smartphone to ensure the Tablet or Smartphone is Encrypted when not in use.

11. *External Drives*: Employees may not handle Protected Information on an External Drive.

12. *Remote Access*: Employees should handle Protected Information maintained on NHRS Information Systems using an Electronic Device outside of NHRS' firewall (including a personal Electronic Device) only if they do so (a) through the dual authentication system maintained by NHRS, and (b) the transmission is Encrypted.

13. *Usernames, Passwords, and Security Codes*: Employees should not use the username, password, or security code of any other Person to access any NHRS security system, facility, Information System, or Electronic Device, or handle any Protected Information. Employees should not permit any other Person to use their username, password, or security code to access any NHRS security system, facility, Information System, or Electronic Device, or handle any Protected Information.

14. *Destruction and Disposal*: Employees should dispose of Protected Information in hard copy format only as required under paragraph II, E.2. Employees should dispose of and destroy Protected Information in electronic format, and Information Systems that contain Protected Information, only as required under paragraph II, D.15.

15. *Data Incidents*: Employees should not engage in any conduct that they know or suspect may result in any actual or expected threat to Protected Information. Employees should inform the Executive Director or Director of IT if they have reason to believe that any actual or threatened Incident has occurred, will occur, or may occur. Employees are expected to cooperate with all investigations and other measures to address any actual or threatened Incident to Protected Information.

16. *Questions and Concerns*: Employees should inform the Executive Director or the Director of IT of any question or concern they have about Protected Information, this Policy, or Applicable law.

17. *Cooperation and Participation*: Employees are expected to cooperate and comply with all practices, procedures, policies, programs, systems, and other measures under this Policy or others implemented by NHRS to safeguard Protected Information.

18. Discipline: Employees will be subject to discipline, which may include termination of employment, for failing or refusing to comply with this Policy, Applicable Law, or any related request or instruction made by NHRS.

C. <u>Administrative Safeguards</u>

1*. Risk Assessments and Policy Review*: The Director of IT is expected to initiate and direct a periodic assessment to determine what Protected Information NHRS has, whether to modify or expand the scope of Protected Information, whether NHRS is subject to any new, additional or reoccurring risks to Protected Information, whether NHRS should implement any new or additional measures to mitigate such risks, and, if so, the measures that NHRS should implement. Based on that assessment, the Executive Director or designee is expected to take steps to implement the measures that NHRS determines it should implement and to modify and amend this Policy if necessary or appropriate. The Executive Director and designee(s) will maintain records memorializing the assessments performed by NHRS and any other matters related to this Policy.

2*. Employee Training*: NHRS is expected to periodically train Employees and provide refresher trainings to Employees about their authority and responsibility under this Policy and Applicable Law and about other topical information related to the safeguarding of Protected Information and the avoidance of actual and threatened Breach. During the orientation of each new Employee, the Director of IT or designee(s) will train Employees concerning their authority and responsibility under this Policy and Applicable Law. The Director of IT and Human Resources Manager will maintain records of such trainings.

3*. Data Contractors*: Before NHRS retains any Person to be a Data Contractor, the Director of IT is expected to determine whether, and the extent to which, NHRS must or should conduct due diligence with respect to such Person given the nature and scope of the Person's anticipated handling of Protected Information and is expected to direct such due diligence. Before providing Protected Information to any Data Contractor, the Director of IT is expected to confirm that NHRS has an appropriate written data security agreement or provision with the Data Contractor. If, or to the extent, any Data Contractor has access to, or responsibilities for, Protected Information that changes materially, the Director of IT is expected to reassess the factors identified above and determine whether any additional due diligence or a modified data security agreement is necessary or appropriate.

4*. Data Incident Response*: In the event of any actual or threatened data incident, the Executive Director or designee will initiate and direct a process to (a) determine if an Incident occurred and, if so, the nature and extent of Protected Information affected; (b) identify the individuals affected by the Incident and Persons that NHRS should notify about the Incident; and (c) determine if NHRS should implement measures to mitigate any risk to Protected

Information related to the Incident or any other risk discovered during the process and, if so, implement such measures.

5. Record Retention. The Executive Director or designee should ensure that NHRS retains all records and other information that are required, necessary, or appropriate to be retained under this Policy or Applicable Law after the creation of the record or other information for a period timed as determined by the Executive Director or designee(s).

6. Insurance: NHRS should maintain commercially reasonable insurance providing appropriate types and levels of coverage for a Data Incident, with regard to Protected Information.

D. Technical Safeguards

1. Director of IT: The Director of IT has authority and responsibility to (a) interpret, implement, and enforce this Policy related to safeguards, (b) develop additional and supplemental policies concerning safeguards, (c) develop, implement, and enforce existing, new, and additional security practices about safeguards, and (d) generally ensure compliance with this Policy and Applicable Law related to safeguards.

2. Access Limitations: NHRS limits access to Protected Information in electronic format to only those Employees who need access to such Protected Information to perform their duties for NHRS. The Director of IT will implement a system of limiting Employee access to Protected Information in NHRS' Information Systems.

3*. Laptops and External Drives*: NHRS provides Laptops to Employees who need Protected Electronic Information on a Laptop to perform their duties for NHRS. The Director of IT will ensure that (a) a Strong Password is required to access the Laptop or the Protected Information on it, and (b) the entire Laptop or the Protected Information on it, is Encrypted.

4*. Tablets and Smartphones*: The Director of IT should implement technological controls in an effort to ensure that any Employee who accesses an NHRS email account using a Tablet or Smartphone, including a personal Tablet or Smartphone, is required to use a Strong Password or Biometric Identifier to ensure that the Tablet or Smartphone is Encrypted when not in use.

5*. Usernames and Passwords or Biometric Identifiers*: Employees are expected to have a unique username and a Strong Password or Biometric Identifier to access NHRS Information Systems and Electronic Devices. The Director of IT will direct Employees to change such passwords at least once every 180 days. The Director of IT will work to ensure that NHRS Information Systems and Electronic Devices have software implemented that requires the use of the Strong Password or Biometric Identifier to access the device if it has not been used for 15 minutes or longer. Promptly after an Employee ceases to be employed by NHRS, NHRS will revoke each of that Employee's usernames, passwords, and Biometric Identifiers. NHRS also will revoke the usernames, passwords, and Biometric Identifiers for any Employee as soon as NHRS becomes aware that the Employee presents a threat to the security of Protected Information.

6. *Remote Access*: NHRS has a virtual private network with dual authentication that permits the handling of Protected Information using an Electronic Device outside of NHRS' firewall. All handling of Protected Information by any Person using an Electronic Device outside of NHRS' firewall shall only occur through that virtual private network.

7. *Issuance and Inventory*: The Director of IT is expected to maintain an inventory of all NHRS Electronic Devices issued to Employees. Before issuing any Electronic Device to an Employee, the Director of IT will ensure that all Protected Information on the Electronic Device is removed from it in accordance with industry standards as determined to be necessary or appropriate by the Director of IT.

8. *Information Systems*: All network infrastructure that supports NHRS' Information Systems and contain Personal Information should be maintained either in a secure facility controlled by NHRS or offsite with a Data Contractor. The Director of IT is expected to confirm that NHRS conducts appropriate due diligence with such Data Contractors in accordance with paragraph II, C.3.

9. *Software Updates*: To the extent feasible, NHRS uses the automatic updating functionality of commercially available software on NHRS' Information Systems. If not feasible, the Director of IT is expected to ensure that, no less than once every month, NHRS manually updates commercially available software on NHRS Information Systems.

10. *Protective Software:* NHRS is expected to maintain up-to-date, commercially reasonable software and systems to safeguard Protected Information, including firewall, anti-virus, anti-malware, and anti-spyware software. NHRS is expected to maintain software and systems that detect, and protect against, multiple failed attempts to log-on to NHRS' Information Systems and disable the account being used to attempt to log-on.

11. *Logs*: NHRS will implement and maintain up-to-date, commercially reasonable software and systems that log the handling of Protected Information in the NHRS Information Systems, and will maintain those logs for the period of time that the Director of IT determines is appropriate or necessary under the circumstances.

12. *Administrators and Software Installation*: Employees generally are not administrators of any of NHRS Information System or Electronic Device. Only the Director of IT or designees may be an administrator of a NHRS Information System or Electronic Device. Administrator usernames and passwords are given to the Director of IT and, if stored electronically, are Encrypted. Employees, including administrators, may not download executable software to NHRS Information Systems or Electronic Devices without prior express approval of the Director of IT.

13. *Transmission of Protected Information*: NHRS has implemented and maintains technology that enables the transmission of Protected Information in electronic format, including by email and by file transfer protocol, pursuant to industry standards.

14. *Transportation of Protected Information*: NHRS has implemented and maintains technology that enables the transportation of Protected Information on Electronic Devices, including Laptops, External Drives, Tablets, and Smartphones, pursuant to industry standards.

15. *Destruction of Protected Information*: If NHRS destroys electronic Protected Information, or Information Systems or Electronic Devices containing such Protected Information, the Director of IT will confirm such destruction conforms to industry standards. If NHRS retains a Data Contractor to destroy electronic Protected Information, or Information Systems or Electronic Devices containing such Protected Information, the Director of IT will confirm in the contract or agreement with the Data Contractor that such destruction conforms to industry standards.

16. *Disaster and Emergency*: NHRS creates and maintains back-ups of Protected Information in electronic format; can restore and use Protected Information in electronic format within a reasonable time after a natural or other disaster affecting NHRS Information Systems; and can continue critical business operations involving electronic Protected Information, during and after an emergency or mass failure of NHRS Information Systems.

E. <u>Physical Safeguards</u>

1*. Facility Security*: Access to NHRS' physical facilities is limited to Employees and other Persons with authority to access such facilities. During non-working hours, NHRS' physical facilities are protected by security systems. Promptly after an Employee ceases to be employed by NHRS, NHRS recovers all access codes, cards, and keys from the Employee.

2*. Disposal and Destruction of Protected Information*: NHRS provides Employees with locked receptacles for the disposal of Protected Information in hard copy format. NHRS has retained a Data Contractor to destroy Protected Information in hard copy format and contractually requires the Data Contractor to destroy it in a manner that renders it essentially unreadable and indecipherable, such as by shredding, burning, or pulverizing.

.