NYSERDA External Contractors
Data Classification and Security Controls Policy

Revision History

Version Number	Date Published	Revision Description

4	2-6-2020	• Updated the definition of Confidential-Private to include interagency staff
		• Updated Data Classification of LSR Bid Price
		  • LSR Awarded Price is classified as Public for executed contracts.
		  • LSR bid price in **non-awardee** proposals is classified as Confidential-Private for five years
		• Added HTTPS Web Portal as an example of a NYSERDA Secure File Transfer Protocol (SFTP)
		• Added Qualtrics as an example of a Secured Database
		• Removed Skype for Business; Microsoft Teams should be used

3	8-5-2019	• Added language that Data Governance, Information Technology, and Information Security must approve all new software products before downloading or executing a contract
		• "Accepted upon Approval" has been added for the following platforms
		  • Encrypted email to an external email account for Confidential-Restricted information
		  • Email to/from an external email account for Confidential-Internal or Confidential-Private information
		  • Fax to Physically Secure Fax for Confidential-Internal, Confidential-Private, or Confidential-Restricted
		• New Examples of Storage/Sharing Platforms or Data
		  • OTDA referral as an example of Confidential-Restricted data
		  • Customer utility data accessed through Electronic Data Interchange as an example of Confidential-Restricted
		  • Accion (LSR) as an example of 'Encrypted and Secured Database'
		  • External Tableau dashboards as an example of 'NYSERDA Public facing Website'
		• Doodle Poll has been added as a Prohibited platform to initiate a Doodle Poll. Microsoft Forms should be used. Responding to Doodle Polls is ok as long as you do not sign in with your NYSERDA Microsoft Office 365 account.

2	2-12-2019	• Revised classification definitions and access • Email outside NYSERDA may include limited residential customer contact information (last name and application number, or last name and phone number) when requested by the residential customer, and when conducting business with a contractor or another authorized external stakeholder such as a utility • Residential customer contact lists are NOT allowed in emails outside NYSERDA • Updated language for sharing data governed by a Confidentiality Agreement and/or Non-Disclosure Agreement (NDA) • Executed contracts are classified as Public, unless marked as Confidential. NYSERDA does not publish this information; NYSERDA would release the information under a FOIL request

Version Number	Date Published	Revision Description

		• Mini bids are classified as Public. Email may be used to send proposals to contractors
		• All completed scoring sheets are classified as Confidential-Private (even for mini bids)
		• New Platforms Added to Table:
		  • **Encrypted & Secured Local Area Network Drive** *(Conf-Private, Conf-Restricted)*
		  • **Non-NYSERDA External SharePoint Sites** *(Not Allowed)*
		  • **Personal Email Accounts** *(Not Allowed)*
		  • **Salesforce Chatter** *(Public and Conf-Internal)*
		  • **Scan to Encrypted Folder with Xerox Workflow Scanning** *(Public, Conf-Internal, Conf-Private)*
		  • **Fax to Physically Secure Fax** (*Public; for Conf-Internal, Conf-Private and Conf-Restricted approval is needed*)
		  • **Print from Mobile Device to xeroxmp@nyserda.ny.gov** *(Public and Conf-Internal)*
		  • **Thumb Drive with AES 256-bit level encryption** *(Public, Conf-Internal, Conf-Private, Conf-Restricted)*
		  • **Skype for Business** *(Public and Conf-Internal)*
		  • **Investment Management software** *(Public, Conf-Internal, Conf-Private, Conf-Restricted)*
		  • **Encrypted email** *(Public, Conf-Internal, Conf-Private)*

1	11-22-2017	First release of Data Classification and Security Controls Policy

Purpose and Benefits of this Document

The New York State Energy and Research Development Authority (NYSERDA) has adopted a Data Classification and Security Controls policy that was first approved by NYSERDA's Data Governance Council on October 2, 2017. The policy describes how to receive, share, and store data and documents based on the sensitivity (classification) of the data. All departments across the Authority, and contractors conducting work on behalf of NYSERDA, are required to comply with the policy in order to manage information entrusted to NYSERDA and its contractors in a way that uniformly protects confidentiality so that the risk of inappropriately releasing or inadvertently providing access to certain information is reduced to an acceptable level.

I. Data Classification Process

NYSERDA classifies all data elements and data assets based on the confidentiality principle of security. A data element is an individual attribute or data point with a precise meaning that helps define, describe, and classify processes and entities (people, places, and things) and their relationships. A data asset is a collection of data elements that is stored or distributed as a single entity (document, report, email, dataset, or database record).

II. Data Classifications Types and Definitions

NYSERDA follows the New York State Information Classification Policy (NYS-S14-002), which mandates that all data must be classified based on three principles of security: confidentiality, integrity, and availability. This document supplements the New York State Information Classification Policy (NYS-S14-002) and describes the classification types NYSERDA will use for the confidentiality principle of security only. This document does not describe the classification types for the integrity and availability principles. The confidentiality classifications are described in the chart below.

Data Classification Types and Definitions

The examples provided below are *examples-only*. If a NYSERDA Confidentiality Agreement and/or Non-Disclosure Agreement (NDA), as stand-alone or as part of a broader contract, exists with an external stakeholder/third party or information assets entrusted to NYSERDA are governed by an MOU, NDA, or Confidentiality Agreement, NYSERDA's compliance obligations are with respect to the stated restrictions on acceptable methods of communication therein regardless of whether it's more or less restrictive than the Data Classification and Security Controls Policy. Every effort should be made to comply with this policy; please request approval from Counsel and Data Governance before entering into an Agreement that is inconsistent with this policy.

Classification	Definition & Access	Impact of Unauthorized Access or Disclosure	NYS Information Classification Category	Disclosed Under Freedom of Information Law (FOIL)	Examples These are examples-only; if an NDA, MOU or other agreement exists, the classification must comply with the stated restrictions
Public	Freely available, unrestricted, and released to the public as appropriate. (Classifying data and information as Public does not mean it must be shared or posted on NYSERDA's web site)	No impact on NYSERDA, its critical functions, workforce or stakeholders	Low	Yes	Non-residential contact information; project city, state, and zip; contractor name; project cost; incentive amount; energy savings; nameplate capacity; LSR awarded bid price in post executed contracts; post executed contracts unless marked as confidential (including draft versions of the Statement of Work); mini bids (mini bids are part of the task work order process for contractors competitively selected for umbrella contracts); and transaction profiles
Confidential-Internal	Approved for NYSERDA and external stakeholders with defined access; not approved for public circulation. Accessible to and used by NYSERDA employees (full-time, part-time and interns) without restriction in the performance of their job duties. Can be made accessible to Non-NYSERDA employees (staff augmentation, contractors, and temporary staff) and interagency staff when required for the performance of their job duties. Under specific circumstances, can be made accessible to other external stakeholders.	Limited or no impact on NYSERDA, its critical functions, workforce, and stakeholders, and is unlikely to result in financial loss, or serious credibility damage	Moderate	May be disclosed; subject to a case-by-case determination	Residential customer name, street address, email, and phone number; draft solicitations/RFP's; and Operations and Procedures Manuals (NYSERDA and NYGB)
Confidential-Private	Deemed to be of a sensitive, private, or confidential nature by federal law or regulation, State law or regulation, or NYSERDA policy or agreement. The preservation of confidentiality is required to the extent permitted by law. Accessible to and used by authorized NYSERDA employees (full-time, part-time, and interns) without restriction in the performance of their job duties. Can be made accessible to Non-NYSERDA employees (staff augmentation, contractors, temporary staff, and interagency staff) when required for the performance of their job duties. Under specific circumstances, can be made available to other external stakeholders.	Serious impact on NYSERDA, its critical functions, workforce, or stakeholders	High	May be exempt from disclosure; subject to a case-by-case determination	Utility account number; proposals under review by the scoring committee[1]; completed score sheets (including completed score sheets for mini bids); LSR bid price for non-awardee proposals (5 years); non-anonymized survey responses; energy usage and price data for commercial and industrial customers; LSR raw bid data; intellectual property if marked confidential by the proposer; information subject to NDA Confidentiality Provision in loan and credit agreements; and applicant resumes and cover letters
Confidential-Restricted	Deemed to be of a highly sensitive nature by federal law or regulation, State law or regulation, or NYSERDA policy or agreement and therefore is only released on a need-to-know basis. Restricted to a very limited set of authorized NYSEDRA employees (full-time, part-time, and interns) as required by federal law or regulation, State law or regulation, or NYSERDA policy or agreement. Can be made accessible to Non-NYSERDA employees (staff augmentation, contractors, and temporary staff) when required for the performance of their job duties. Under specific circumstances, can be made available to other external stakeholders.	Severe or catastrophic impact on NYSERDA, its critical functions, workforce, and stakeholders	High	Likely to be exempt from disclosure; subject to a case-by-case determination	Employee medical documents, social security numbers, and bank account numbers, OTDA referrals per MOU, and Customer Utility Data obtained via Electronic Data Interface (EDI)

1 Specific paragraphs in proposals must be marked as Confidential at time of submittal to be considered proprietary or trade secret information.

III. Data Security and Access and Storage Controls Based on Classification Types

The Data Classification and Security Controls Policy delineates how data may be shared or stored corresponding to the type of data classification—for example, Public, Confidential-Internal, Confidential-Private, and Confidential-Restricted.

How and where data can be shared or stored?

The preferred and allowed data sharing and storage platforms for each data classification type are shown in the Data Access and Storage Controls Policy table at the end of this document.

Below are known platforms that are PROHIBITED to collect, share, or store data. This is not an exhaustive list.

- Non-NYSERDA External SharePoint Site
- Third-party solutions to upload files from a non-NYSERDA to a NYSERDA External SharePoint
- Personal email accounts (including but not limited to Gmail, Yahoo, Hotmail, AOL)
- Cloud Storage Platforms (Dropbox, Drop Box Professional, Google Drive)
- Google Docs
- CD Rom
- Emailing residential customer contact lists outside of NYSERDA
- Doodle Poll (Initiating a Doodle Poll is prohibited. Responding to a Doodle Poll is ok if you do not sign in with your NYSERDA Microsoft Office 365 account)

Data Access and Storage Controls Policy: How and Where Data Can Be Shared or Stored

The examples provided below are *examples-only*. If a NYSERDA Confidentiality Agreement and/or Non-Disclosure Agreement (NDA) (i.e., stand-alone or as part of a broader contract) exists with an external stakeholder/third party or information assets entrusted to NYSERDA are governed by an MOU, NDA, or Confidentiality Agreement, NYSERDA's compliance obligations are with respect to the stated restrictions on acceptable methods of communication therein regardless of whether it's more or less restrictive than the Data Classification and Security Controls Policy. Every effort should be made to comply with this policy; please request approval from Counsel and Data Governance before entering into an Agreement that is inconsistent with this policy. Before contracting to purchase or downloading any software products, please contact Data Governance who will work with Information Security, Information Technology, and Web Development on necessary approvals to ensure the software product complies with NYS security and **Americans with Disabilities Act (ADA)** requirements. Please contact Data Governance for all Accepted Upon Approval requests.

KEY: YES - Recommended Platform **YES – Approved Platform** **NO - Platform Not Approved** **PROHIBITED**

Data Sharing and Storage Platform - Electronic Data	**PUBLIC** **Data Allowed?** *Examples: Project City, State, and Zip; Contractor Name; Project Cost; Incentive Amount; Energy Savings; Nameplate Capacity; Post Executed Contracts Unless Marked as Confidential; LSR awarded bid price in post executed contracts; Mini Bids; Transaction Profiles*	**CONFIDENTIAL-INTERNAL** **Data Allowed?** *Examples: Residential Customer Name, Street Address, Email, and Phone Number; Draft Solicitations and RFP's; Operations & Procedures Manuals*	**CONFIDENTIAL-PRIVATE** **Data Allowed?** *Examples: Utility Account Numbers; Proposals under review by Scoring Committee; Proposals; Completed Scoring Sheets; Non-anonymized Survey Responses; Energy Usage; LSR Bid for non-awardee proposals (5 years);* *Data, Intellectual Property when marked confidential; Loan and Credit Agreements; Applicant Resumes and Cover Letters*	**CONFIDENTIAL-RESTRICTED** **Data Allowed?** *Examples: Customer Utility data obtained through EDI; OTDA Referrals per MOU; Employee Medical Documents; Social Security Numbers; Bank Account Numbers*
Encrypted and Secured Database (Salesforce, Salesforce Deliverable Submission Portal, Accion (LSR), NEIS, Powerclerk, Seamless Docs, ADP, etc.)	YES	YES recommended method for sharing and managing data securely	YES with limited authorized users recommended method for sharing and managing data securely	YES w/ encryption & limited authorized users recommended method for sharing and managing data securely
Secured Database (OACSS, CRIS, Buildings Portal, Qualtrics)	YES	YES	YES with limited authorized users	NO
Encrypted and Secured Local Area Network Drive	NO encryption not required	NO encryption not required	YES with limited authorized users	YES w/ encryption & limited authorized users
Secured Local Area Network Drive	YES	YES	YES with limited authorized users	NO
Non-Secure Local Area Network Drive	YES	YES	NO	NO
NYSERDA External SharePoint Site with Limited Authorized Users	YES recommended method for collaboration	YES recommended method for collaboration	YES recommended method for collaboration	YES recommended method for collaboration
Secure File Transfer Protocol – SFTP (HTTPS web portal, File Zilla)	YES recommended for recurring outgoing or incoming transfers	YES recommended for recurring outgoing or incoming transfers	YES recommended for recurring outgoing or incoming transfers	NO
NYSERDA Web Link with Secured Password Protected Portal	YES	YES recommended for one-time outgoing file sharing	YES recommended for one-time outgoing file sharing	NO
NYSERDA's Public-Facing Websites (nyserda.ny.gov, DG website, external Tableau dashboards)	YES	NO	NO	NO
Third-Party Website (Open NY, CUNY, etc.)	YES Open NY preferred for publishing datasets	NO	NO	NO
Encrypted Email	YES	YES attachments must be password protected[2]	YES attachments must be password protected[2]	ACCEPTED UPON APPROVAL

2 Attachments must be converted to an Adobe or Excel .xlsx password protected file for Confidential-Private data before sending an encrypted email. **Files in the .xls format must be recreated and saved as a new .xlsx file. The .xls format does not meet NYS security requirements and may be hacked.** The password must be changed every 90 days and contain 8 characters of upper/lower case, number and special characters). The password should be provided over the phone or in a separate email. With so many email accounts being compromised at other entities, it is recommended to transmit the password over the phone if possible.

Data Sharing and Storage Platform - Electronic Data	PUBLIC Data Allowed? *Examples: Project City, State, and Zip; Contractor Name; Project Cost; Incentive Amount; Energy Savings; Nameplate Capacity; Post Executed Contracts Unless Marked as Confidential; LSR awarded bid price in post executed contracts; Mini Bids; Transaction Profiles*	CONFIDENTIAL-INTERNAL Data Allowed? *Examples: Residential Customer Name, Street Address, Email, and Phone Number; Draft Solicitations and RFP's; Operations & Procedures Manuals*	CONFIDENTIAL-PRIVATE Data Allowed? *Examples: Utility Account Numbers; Proposals under review by Scoring Committee; Proposals; Completed Scoring Sheets; Non-anonymized Survey Responses; Energy Usage; LSR Bid for non-awardee proposals (5 years);* *Data, Intellectual Property when marked confidential; Loan and Credit Agreements; Applicant Resumes and Cover Letters*	CONFIDENTIAL-RESTRICTED Data Allowed? *Examples: Customer Utility data obtained through EDI; OTDA Referrals per MOU; Employee Medical Documents; Social Security Numbers; Bank Account Numbers*
Email, or Fax	YES	ACCEPTED UPON APPROVAL limited customer contact info allowed[3]	ACCEPTED UPON APPROVAL	NO
Fax to Physically Secure Fax	YES	ACCEPTED UPON APPROVAL	ACCEPTED UPON APPROVAL	ACCEPTED UPON APPROVAL
Investment Management Software (Bank of America Cash Pro, SS&C GlobeOp and Concord Interlink, NYGB Bloomberg Anywhere subscription)[4]	YES	YES	YES	YES
Scan to (Encrypted Xerox Workforce Scanning) Secured Local Area Network Drive	YES	YES	YES with limited authorized users	NO
RightFax (data is stored in US)	YES	YES	YES	YES
Thumb Drive with AES 256-bit level encryption (preferred method is NYSERDA External SharePoint Site)	YES recommended method is NYSERDA External SharePoint Site	YES recommended method is NYSERDA External SharePoint Site	YES recommended method is NYSERDA External SharePoint Site	YES recommended method is NYSERDA External SharePoint Site
Cloud Storage Solutions (Drop Box, Drop Box Professional, Google Drive)	PROHIBITED	PROHIBITED	PROHIBITED	PROHIBITED
Google Docs	PROHIBITED	PROHIBITED	PROHIBITED	PROHIBITED
CD ROM	PROHIBITED	PROHIBITED	PROHIBITED	PROHIBITED
Non-NYSERDA External SharePoint site (Third party solutions to upload files from a Non-NYSERDA to a NYSERDA External SharePoint are also prohibited)	PROHIBITED	PROHIBITED	PROHIBITED	PROHIBITED
Personal email accounts (including but not limited to Gmail, Yahoo, Hotmail, AOL)	PROHIBITED	PROHIBITED	PROHIBITED	PROHIBITED
Doodle Poll (Initiating a Doodle Poll is prohibited. Microsoft Forms is an approved alternative; contact the Service Desk with any questions. Responding to a Doodle Poll is ok if you do not sign in with your NYSERDA Microsoft Office 365 account.)	PROHIBITED Cannot Initiate a Doodle Poll	PROHIBITED Cannot Initiate a Doodle Poll	PROHIBITED Cannot Initiate a Doodle Poll	PROHIBITED Cannot Initiate a Doodle Poll
Data Sharing and Storage Platform - Physical Data (Paper)	**PUBLIC Data Allowed?**	**CONFIDENTIAL-INTERNAL Data Allowed?**	**CONFIDENTIAL-PRIVATE Data Allowed?**	**CONFIDENTIAL-RESTRICTED Data Allowed?**
Mail Services	YES	YES	YES only after authorization	YES only after authorization
Unlocked File Cabinets or Other Unsecure Cabinets	YES	YES	NO	NO
Locked Cabinet within a Secured Storage Facilities or Locked Office (on-site storage located in basement, or off-site, such as Honeywell)	YES	YES	YES secured with limited authorized users	YES secured with limited authorized users

3 Email outside of NYSERDA may include limited residential customer contact information (last name and application number, or last name and phone number) when requested by the residential customer, and when conducting business with a contractor or other authorized external stakeholder, such as a utility. If necessary, customer contact information may be shared if there is no unique identifier when conducting business with the contractor. Legal language must be included in the email when sharing residential customer information – "This electronic message may contain privileged or confidential information. If you are not the intended recipient of this e-mail, please delete it from your system and advise the sender. Residential customer contact lists are NOT allowed in emails outside of NYSERDA."

4 These platforms meet NYS requirements and will be re-evaluated each year.