Data Privacy Policy

New England Municipal Resource Center (NEMRC, I, we, us) has the following data collection practices and policies regarding its company, product offerings and websites.

Overall

The NEMRC overall privacy principle is simple. Unless explicitly stated to a client (A company, elected official or person that uses any NEMRC product or service by agreement.) , any information we receive from a client will not be shared with anyone else, and NEMRC will never use it for anything that is not absolutely necessary to provide its products and services.

NEMRC Company

NEMRC collects the following data with regard to clients: name, contacts, mailing address, phone numbers, email addresses.

NEMRC uses this data for its own business purposes only. The data is not shared with any other company.

NEMRC Desktop Software

NEMRC Desktop Software performs actions on the internet that allow for the collection of the following information: NEMRC site code, IP Address of the request, metadata regarding any backups made to NEMRC servers, metadata regarding updates requested and delivered via the www.nemrc.com website, serious service level messages that are reported to NEMRC support. Service level messages do not contain any personal information.

NEMRC uses this data for its own business purposes only. The data is not shared with any other company.

From time to time NEMRC desktop software will ask clients to share specific information from the NEMRC Desktop Software data files. NEMRC will explicitly state the reason. At the client's discretion they can choose to share that information or NOT. An example would be the number of residential parcels being maintained in CAMA for the purposes of reporting and billing license data to CoreLogic (Marshall and Swift).

There are also specific and explicit software functions that share data with third parties. The purpose of these functions varies, however in all cases are intended to ease the record keeping of the client. Examples would include CoreLogic tax escrow service exports.

At no point will NEMRC software automatically send any information to any third party without an explicit action performed by a NEMRC client to allow for such sharing.

NEMRC Desktop Software and Personally Identifiable Information (PII)

NEMRC desktop software collects and stores data that is considered PII. NEMRC encrypts all PII data while the data is at rest in predefined data files. For a listing of PII data and what modules maintain PII data please see our website and search for PII.

NEMRC Software will only report and display PII data in order to complete its clients business tasks.

Clients ARE, NEMRC Software is NOT, responsible for reports or files created by an action of clients that contain PII once generated by the NEMRC software. Clients should expunge any report or file that contains PII once used for its intended business purpose.

NEMRC On-line Backup Disaster Recovery Assistance (DRA) Services

NEMRC receives and stores encrypted (NEMRC Desktop Software) backups on its server(s) at the request of clients, these backups may be part of a disaster recovery assistance Service Level Agreement (SLA).

NEMRC uses these backups in the following ways.

1. Help clients recover from situations in which their data was lost.
2. Help clients with support related issues.

NEMRC does not share these backups with any other company outside NEMRC.

NEMRC Cloud Services

NEMRC collects and maintains client and workstation data used to offer and administer internet hosting services for its optional cloud service This cloud service is used exclusively to host NEMRC desktop software for NEMRC clients. Data collected includes: clients local login name, clients login name, clients local and remote ip address, one browser “cookie” used explicitly to identify a browser and belonging to a client, and server logs.

NEMRC only uses this data for its own business purposes. The data is not shared with any other company.

Security Of Data

Internet security of your data is important to NEMRC, but no method of transmission over the Internet, or method of electronic storage is 100% secure. NEMRC ensures data is encrypted at least once (if not multiple times) when data is transferred over a public network (internet).

Any data stored on network servers not maintained by NEMRC are not the responsibility of NEMRC. Any breach from such network servers is the responsibility of and should be reported by the owners of that network, not NEMRC.

Transfer Of Data

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside the United States and choose to provide information to us, please note that we transfer the data, including Personal Data, to United States and process it there.

Your consent to this Data Privacy Policy followed by your submission of such information represents your agreement to that transfer.

NEMRC will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Data Privacy Policy and no transfer of your Personal Data will take place to an organization unless there are adequate controls in place including the security of your data and other personal information.

Retention of Data

NEMRC will retain your data only for as long as is necessary for the purposes set out in this Data Privacy Policy. We will retain and use your data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

NEMRC will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this data for longer time periods.

Disclosure Of Data

Disclosure for Law Enforcement

Under certain circumstances, NEMRC may be required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Legal Requirements

NEMRC may disclose your Personal Data in the good faith belief that such action is necessary:

- To comply with a legal obligation
- To protect and defend the rights or property of NEMRC
- To prevent or investigate possible wrongdoing in connection with the Service
- To protect the personal safety of users of the Service or the public
- To protect against legal liability

Children's Data Privacy

Our Services are not addressed to anyone under the age of 13 ("Children"). We do not knowingly collect personally identifiable information from anyone under the age of 13. If you are a parent or guardian and you are aware that your Children have provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

Your Rights

NEMRC aims to take reasonable steps to allow you to correct, amend, delete, or limit the use of your Personal Data. Please contact us (800-387-1110 8:30-4:30 Eastern time weekday non-holiday) to make the required changes.

If you wish to be informed what Personal Data we hold about you please contact us.

Your Personal Data will be deleted upon deletion of your NEMRC web account (if any). Please note, however, that there might be latency in deleting information from our servers and backed-up versions might exist after deletion.

In certain circumstances, you have the right:

- To access and receive a copy of the Personal Data we hold about you
- To rectify any Personal Data held about you that is inaccurate
- To request the deletion of Personal Data held about you

You have the right to data portability for the information you provide to NEMRC. You can request to obtain a copy of your Personal Data in a commonly used electronic format so that you can manage and move it.

Please note that we may ask you to verify your identity before responding to such requests.

Service Providers

We may employ third party companies and individuals to facilitate our Service ("Service Providers"), to provide the Service on our behalf, to perform Service-related services or to assist us in analyzing how our Service is used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

NEMRC Websites

NEMRC only collects data in support of its products and services. Any data that is considered personal in anyway will be encrypted in transit to NEMRC. The following applies to **www.nemrc.com:**

"Do Not Track" Signals

We do not support Do Not Track ("DNT"). Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked. The services provided by NEMRC require that we know who is using our services.

You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

Payments

We do not accept on-line payments via any product or service that NEMRC provides or maintains. More specifically, we do not accept card payments, as such we do not store or collect any card details. We are not required to adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

Links To Other Sites

Our Products or Services may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services. We strongly advise you to review the Privacy Policy of every site you visit.

Analytics

We may use third-party Service Providers to monitor and analyze the use of our Service.

Google Analytics

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising network. You can opt-out of having made your activity on the Service available to Google Analytics by installing the Google Analytics opt-out browser add-on. The add-on prevents the Google Analytics JavaScript (ga.js, analytics.js, and dc.js) from sharing information with Google Analytics about visits activity.

For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page: http://www.google.com/intl/en/policies/privacy/

EU GDPR compliance

NEMRC as a company meets the requirements of the GDPR for its services and networks. Personal data will only be used to provide NEMRC services. Any client of NEMRC should adopt their own GDPR compliance especially those clients that may maintain data for EU citizens.

Model Contract Clauses

NEMRC offers a data-processing amendment and model contract clauses as an additional means of meeting the adequacy and security requirements of the “European Parliament and Council of the European Union Data Protection Directive” when needed. This agreement can be accepted and reviewed after purchasing NEMRC Services. The amendment agreement is below.

Changes to our Data Privacy Policy

This Data Privacy Policy may change from time to time. If we make a change to this policy that we believe materially **reduces** your rights, we will provide you with notice (for example, by email). And we may provide notice of changes in other circumstances as well. By continuing to use the Service after those changes become effective, you agree to be bound by the revised Data Privacy Policy.

Contacting Us

If you have any questions about our Data Privacy Policy, please contact us at support@nemrc.com.

-End of Data Privacy Policy.

Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC

Standard Contractual Clauses (processors)

for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

the non-NEMRC legal entity accepting the Clauses (the "Data Exporter")

And

NEMRC,

PO Box 2020

Fairfax, VT 05468 USA

(the "**Data Importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

The Clauses (including Appendices 1 and 2) are effective from the date the non-NEMRC entity has ordered NEMRC services and any client software. A "Data Processing Amendment" means an amendment to the NEMRC Service Level Support Agreement that sets forth certain terms in relation to the protection and processing of personal data.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '***personal data***', '***special categories of data***', '***process/processing***', '***controller***', '***processor***', '***Data Subject***' and '***Supervisory Authority***' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the ***Data Exporter***' means the controller who transfers the personal data;

(c) 'the ***Data Importer***' means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;

(d) 'the ***Subprocessor***' means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data

exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the ***applicable data protection law***' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;

(f) '***technical and organisational security measures***' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the

relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the Data Importer or any Subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer[1]

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
(d) that it will promptly notify the Data Exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
(ii) any accidental or unauthorised access; and
(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal Data Subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;
(g) to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;
(h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;
(i) that the processing services by the Subprocessor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Subprocessor is entitled to receive compensation from the Data Exporter for the damage suffered.
2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity.The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.
3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent,

the Subprocessor agrees that the Data Subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject;

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
(b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

2. The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.
3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-Processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.
2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.
4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to the Standard Contractual Clauses
This Appendix forms part of the Clauses
Data Exporter

The Data Exporter is the non-NEMRC legal entity that is a party to the Clauses.

Data Importer

The Data Importer is NEMRC, a provider of a variety of technology services for individuals and businesses.

Data Subjects

The personal data transferred concern the following categories of data subjects: the Data Exporter's end users including employees and contractors; the personnel of the Data Exporter's customers, suppliers and subcontractors; and any other person who transmits data via the "Services" (as defined in the Data Processing Amendment) including individuals collaborating and communicating with the Data Exporter's end users.

Categories of data

The personal data transferred concern the following categories of data: personal data submitted, stored, sent or received by the Data Exporter or its end users via the Services including name, address, physical location, property information, and other electronic data stored, sent or received by end users via the Services.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: data submitted, stored, sent or received by end users via the Services.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Scope of Processing.

The Clauses reflect the parties' agreement with respect to the processing and transfer of personal data specified in this Appendix pursuant to the provision of the Services.

Personal data may be processed for the following purposes: to provide the Services and related technical support services.

The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or any of its Subprocessors maintains facilities.

Term of Data Processing.

Data processing will be for the term specified in the Data Processing Amendment. Such term will automatically terminate upon the deletion by the Data Importer of all data as described in the Data Processing Amendment.

Data Deletion.

During the term of the Services Agreement, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter's personal data from the Services in accordance with the Services Agreement. After termination or expiry of the Services Agreement, the Data Importer will delete the Data Exporter's personal data in accordance with the Services Agreement.

Access to Data.

During the term of the Services Agreement, the Data Importer will provide the Data Exporter with access to and the ability to correct, block and export the Data Exporter's personal data from the Services in accordance with the Services Agreement.

Subprocessors.

The Data Importer may engage Subprocessors to provide parts of the Services and related technical support services. The Data Importer will ensure Subprocessors only access and use the Data Exporter's personal data to provide the Services and related technical support services and not for any other purpose.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer currently takes and implements the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the Services Agreement.

1. Data Center & Network Security.

(a) Data Centers.

Infrastructure. The Data Importer maintains geographically distributed data centers. The Data Importer stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow the Data Importer to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. The Data Importer servers use a Windows and or Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. The Data Importer employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments. The Data Importer replicates data over multiple systems to help to protect against accidental destruction or loss. The Data Importer has designed its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers.This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. The Data Importer transfers data via Internet standard protocols.

External Attack Surface. The Data Importer employs multiple layers of network devices and intrusion detection to protect its external attack surface. The Data Importer considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. The Data Importer's intrusion detection involves

1. Tightly controlling the size and make-up of the Data Importer's attack surface through preventative measures;
2. Employing intelligent detection controls at data entry points; and
3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. The Data Importer monitors a variety of communication channels for security incidents, and the Data Importer's security personnel will react promptly to known incidents. Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available.

2. Access and Site Controls.

(a) Site Controls.

On-site Data Center Security Operation. The Data Importer's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. The Data Importer maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and

internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. The Data Importer's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. The Data Importer has, and maintains, qualified personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents. Access Control and Privilege Management. The Data Exporter's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator

Internal Data Access Processes and Policies – Access Policy. The Data Importer's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.The Data Importer employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide the Data Importer with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. The Data Importer requires the use of unique user IDs, strong passwords, and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with the Data Importer's internal data access policies. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability.

3. Data.

(a) Data Storage, Isolation & Authentication.

The Data Importer stores data in a multi-tenant environment on the Data Importer-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. The Data Importer logically isolates data on a per end user basis at the application layer. The Data Importer logically isolates the Data Exporter's data, and logically separates each end user's data from the data of other end users, and data for an authenticated end user will not be displayed to another end user (unless the former end user or an administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data. The Data Exporter will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable the Data Exporter to determine the product sharing settings applicable to end users for specific purposes. The Data Exporter may choose to make use of certain logging capability that the Data Importer may make available via the Services, products and APIs. The Data Exporter agrees that its use of the APIs is subject to the API terms of use. The Data Importer agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) Decommissioned Disks and Disk Erase Policy.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving the Data Importer's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security.

The Data Importer's personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (eg., certifications). The Data Importer's personnel will not process customer data without authorization.

5. Subprocessor Security.

Prior to onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

6. Data Privacy Officer.

The Data Privacy Officer of the Data Importer can be contacted by the Data Exporter's Administrators at: support@NEMRC.com (or via such other means as may be provided by the Data Importer).

[1]Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Rev. 1 Adopted by NEMRC 11/27/2019