# BREACH RESPONSE AND NOTIFICATION POLICY

## DEFINITIONS

| | |
|---|---|
| WACG | means the WACG Inc., a company behind the Project Data Suite (projectdata.io) |
| Breach | Breach means the acquisition, access, use, or disclosure of Non-Public or Personally Identifiable in a manner not permitted under relevant laws or regulations, which compromises the security or privacy of the protected information. |
| Business Associate | A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected information (NPI or PII) on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. |
| Covered Entity | For NPI, covered entities are any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law. For PII, any organization, individual and/or individuals who use, store, destroy, transmit, copy, etc. Personally Identifiable Information. |
| Encryption or encrypted data | The most effective way to achieve electronic information security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text |
| Plain text | Unencrypted data. |
| Hacker | A slang term for a computer expert/enthusiast with demonstrated skills in programming languages, computer systems and social engineering, and can often be considered an expert on the subject(s). |
| Non-Public Information (NPI) | Defined as all electronic information that is not publicly available information and is:<br>• Business-related information<br>• Information concerning an individual, which, because of name, number, personal mark or other identifier, can be used to identify such an individual when combined with SSN, driver's license, account number, security code or biometric records |
| Personally Identifiable Information (PII) | Any information that can be used to contact, locate or identify a specific individual, either by itself or combined with other sources that are easily accessed. It can include information that is linked to an individual through financial, medical, educational or employment records. Some of the data elements that might be used to identify a certain person could consist of fingerprints, biometric data, a name, telephone number, email address or social security number. Safeguarding PII and other sensitive information is the responsibility of federal agencies. |
| Protected information | See NPI or PII |
| Information Resource | The data and information assets, both physical and electronic, of an organization, department or unit. |
| Safeguards | Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset. |
| Sensitive information | Information that is encrypted or in plain text and contains NPI or PII. See NPI or PII above. |

## OVERVIEW

This policy mandates that any individual who suspects that a theft, breach or exposure of WACG Protected or Sensitive information has occurred must immediately provide a description of what occurred via email to support@projectdata.io or by calling +1 (256) 667-5724. This e-mail address and phone number are monitored by the WACG 's CTO, Oleg Snurnykov. They will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the CTO will follow the appropriate procedure in place.

## PURPOSE

The purpose of the policy is to establish the goals and the vision for the breach response and notification process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the

incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve information privacy and security protection.

WACG_'s intentions for publishing a Breach Response and Notification Policy are to focus significant attention on information security and information security breaches, and how WACG_'s established culture of openness, trust and integrity should respond to such activity. WACGInformation Security is committed to protecting WACG's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

## SCOPE

This policy applies to all who collect, access (or have access to), maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle non-public (NPI) or personally identifiable (PII) of WACG_and/or its clients. Any agreements with vendors will contain language similar and/or reference this policy, with attestations as to have read, understand and agree to comply with the same.

## POLICY

### Confirmed theft, data breach or exposure of WACG_Protected or Sensitive information

- As soon as a theft, data breach or exposure containing WACG_Protected or Sensitive information is identified, the process of removing all access to that resource will begin.
- The CTO will chair an incident response team to handle the breach or exposure.
- Confirmed theft, breach or exposure of WACG
    - The CTO will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.
    - Notification by any third party provider engaged by WACG_who collects, accesses (or has access to), maintains, distributes, processes, protects, stores, uses, transmits, disposes of, or otherwise handles non-public (NPI) or personally identifiable (PII) to the CTO of the theft, breach or exposure is a requirement of doing business with WACG. The CTO will treat this the same as if it were a breach of WACG; effectively this is out-sourcing the work while in-sourcing the liability. All policies and procedures relating thereto will be followed.
- Work with Forensic Investigators
    - As provided by WACG's cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of information involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.
    - Where WACG's insurance policies don't direct or otherwise cover forensics, unless same is deemed necessary by WACG's CTO, or, if the CTO does not have the authority, the person responsible for such a decision, or required by law, no additional forensics will be performed beyond that of the work done by the Breach Response team.
- Develop a communication plan.

- Work with WACG communications to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.
- As required by relevant laws and regulations, notification of a breach, and the potential, or realized, exposure of NPI/PII, to clients/customers is required.
- Any breach to a third party provider, and who, as required, notified the CTO will, like any breach to WACG will require a Communication Plan per this section. The responsibility for the third party provider is to notify WACG if they've suffered, or believed to have suffered, a data breach. WACG is still liable to disclose the breach to its customers. The responsibility for the third party provider is to notify WACG if they've suffered, or believed to have suffered, a data breach. WACG is still liable to the disclosure of the breach to its customers/clients.

- Delay of Notification
  - Authorized for Law Enforcement Purposes. If a law enforcement official states to the Covered Entity or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Covered Entity or a business associate shall:
    - If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
    - If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

## ENFORCEMENT

- Any WACG personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment.
- Any third party partner company found in violation may have their network connection terminated and/or our relationship severed; the terms of the same to be defined in the Agreement memorializing such relationship.