RISK ASSESSMENT POLICY

DEFINITIONS

WACG	means the WACG Inc., a company behind the Project Data Suite (projectdata.io)
Risk	Those factors that could affect confidentiality, availability, and integrity of WACG's key information assets and systems.

INTRODUCTION

At WACG we consider risk management an integral part of a company's operations.

PURPOSE

To empower Infosec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

SCOPE

Risk assessments can be conducted on any entity within WACG or any outside entity that provides services to the WACG. RAs can be conducted on any information system, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

POLICY

The execution, development and implementation of remediation programs is the joint responsibility of the whole WACG team and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Risk Assessment Team in the development of a remediation plan.

For additional information, see *Appendix A, Risk Assessment Process*.

POLICY COMPLIANCE

Compliance Measurement

The WACG Exec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the WACG Exec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPENDIX A, RISK ASSESSMENT PROCESS.

The following is a high-level overview of the process used by WACG to assess and manage information security-related risks.

STEP 1: PREPARE FOR THE ASSESSMENT

In this step, the objective is to establish the context for the risk assessment. This can be accomplished by performing the following:

- Identify the purpose of the assessment
  - Determine the information that the assessment is intended to produce and the decisions the assessment is intended to support.
- Identify the scope of the assessment
  - Determine the organizational function or process that is applicable, the associated time frame any applicable architectural or technological considerations.
- Identify any assumptions or constraints associated with the assessment
  - Determine assumptions in key areas relevant to the risk assessment including:
  - Organizational priorities
  - Business objectives
  - Resource availability
  - Skills and expertise of risk assessment team
- Identify sources of information
  - Architectural / technological diagrams and system configurations
  - Legal and regulatory requirements
  - Threat Sources
  - Threat Events
  - Vulnerabilities and influencing conditions
  - Potential Impacts
  - Existing Controls

STEP 2: CONDUCT THE ASSESSMENT

In this step, the objective is to produce a list of information security-related risks that can be prioritized by risk level and used to inform risk response decisions. This can be accomplished by performing the following:

- Identify Threat Sources
  - Determine and characterize threat sources relevant to and of concern to WACG, including but not limited to:
    - Human (Intentional or Unintentional / Internal or External)
    - Environmental
    - Natural
    - System or Equipment
  - Consider the following when identifying threat sources:
    - Capability
    - Motive / Intent
    - Intentionally targeted people, processes, and/or technologies
    - Unintentionally targeted people, processes, and/or technologies

- Identify Threat Events
    - Determine what threat events could be produce by the identified threat sources that have potential to impact WACG .
    - Consider the relevance of the events and the sources that could initiate the events.
- Identify Vulnerabilities
    - Determine the vulnerabilities with the WACG such associated to people, process and/or technologies that could be exploited by the identified threat sources and threat events.
    - Consider any influencing conditions that could affect and aid in successful exploitation.
- Determine Likelihood
    - Determine the likelihood that the identified threat sources would initiate the identified threat events and could successfully exploit any identified vulnerabilities.
    - Consider the following when determining the likelihood:
        - Characteristics of the threat sources that could initiate the events.
            - Capability
            - Motive/Intent
            - Opportunity
            - The vulnerabilities and/or influencing conditions identified
            - WACG 's exposure based on any safeguards/countermeasures planned or implemented to prevent or mitigate such events.
- Determine Impact
    - Determine the impact to WACG 's business objectives, operations, assets, individuals, customers, and/or other organizations by considering the following:
        - Business / Operational Impacts
        - Financial Damage
        - Reputation Damage
        - Legal or Regulatory Issues
    - When determining impact, also take into consideration any safeguards/countermeasures planned or implemented by WACG that would mitigate or lessen the impact.
- Determine Risk
    - Determine the overall information security-related risks to WACG by combining the following:
        - The likelihood of the event occurring.
        - The impact that would result from the event.
    - The risk to WACG is proportional to the likelihood and impact of an event.
        - Higher Risk Event: Is more likely to occur and the resulting impact will be greater.
        - Lower Risk Event: Is less likely to occur and the resulting impact will be minimal if any.

STEP 3: COMMUNICATE AND SHARE THE RISK ASSESSMENT RESULTS

In this step, the objective is to ensure that decision-makers across the WACG and executive leadership have the appropriate risk-related information needed to inform and guide risk decisions.

- Communicate the Results
  - Communicate the risk assessment results to WACG decision maker and executive leadership to help drive risk-based decisions and obtain the necessary support for the risk response.
  - Share the risk assessment and risk-related information with the appropriate personnel at WACG to help support the risk response efforts.

STEP 4: MAINTAIN THE ASSESSMENT

In this step, the objective is to keep current, the specific knowledge related to the risks that WACG incurs. The results of the assessments inform, and drive risk-based decisions and guide ongoing risk responses efforts.

- Monitor Risk Factors
  - Conduct ongoing monitoring of the risk factors that contribute to changes in risk to WACG 's business objectives, operations, assets, individuals, customers, and/or other organizations.
- Maintain and Update the Assessment
  - Update existing risk assessments using the results from ongoing monitoring of risk factors and by conducting additional assessments, at minimum annually.