GOLD CIRCLE
INVESTMENTS LTD
Lasting Partnerships

Security Policy

DOC NO: POL-H3SEQ-005-V2

Contents

1. Introduction

Security is paramount for Gold Circle Investments Ltd to ensure the confidentiality, integrity, and availability of our assets, information, and operations. This Security Policy outlines the principles, guidelines, and procedures that all employees, contractors, and stakeholders must adhere to to maintain a secure environment.

2. Security Objectives

- Ensure the protection of sensitive information related to company operations, clients, and partners.
- Safeguard physical assets including vehicles, charging stations, and infrastructure.
- Mitigate risks associated with cyber threats, data breaches, and unauthorized access.
- Foster a culture of security awareness and compliance among all employees and stakeholders.

3. Physical Security

- Implement access controls to restrict entry to facilities, charging stations, and storage areas.
- Utilize surveillance systems to monitor premises and deter unauthorized activities.
- Securely store keys, access cards, and other physical access devices.
- Conduct regular inspections and maintenance of physical security measures.
- Implement procedures for visitor management and escorting guests within company premises.

4. Information Security

- Classify and label all sensitive information according to its level of confidentiality.
- Enforce access controls and user authentication mechanisms to prevent unauthorized access to digital assets.
- Encrypt sensitive data both in transit and at rest.
- Implement robust password policies and encourage the use of multi-factor authentication.
- Regularly update and patch software systems to address vulnerabilities.

5. Cybersecurity

- Deploy firewalls, intrusion detection systems, and antivirus software to protect against cyber threats.
- Conduct regular vulnerability assessments and penetration testing to identify and remediate security weaknesses.
- Educate employees on common cyber threats such as phishing attacks and social engineering tactics.
- Enforce strict policies regarding the use of company-issued devices and access to corporate networks.
- Establish procedures for incident response and recovery in the event of a cybersecurity breach.

6. Employee Responsibilities

- All employees must undergo security awareness training upon joining the company and annually thereafter.
- Employees are responsible for safeguarding company assets, information, and intellectual property.
- Any suspected security incidents or breaches must be reported immediately to the designated security officer.
- Employees must comply with all security policies and procedures outlined in this document.

7. Compliance

- Ensure compliance with relevant legal and regulatory requirements related to security and data protection.
- Regularly review and update security policies and procedures to address evolving threats and risks.
- Conduct periodic audits and assessments to verify compliance with security policies and standards.

8. Conclusion

Security is a shared responsibility and requires the active participation of every employee and stakeholder. By adhering to the principles outlined in this Security Policy, we can mitigate risks, protect our assets, and maintain the trust of our clients and partners. Failure to comply with these policies may result in disciplinary action, up to and including termination of employment or contract.

Annexures

Annexure A: Employee Security Survey Form

EMPLOYEE SECURITY SURVEY

This survey will help detect Security Problems in your building or at an alternate worksite.

Please fill out this form and submit it to ____.

It will be reviewed to help determine where the potential for major security problems lie. NAME: ____

WORK LOCATION: ____

Check Y (yes) or N (no) for all the situations or conditions in your workplace that may be associated with causing an unsafe worksite:

___ There is a written policy to follow for addressing general security problems.

___ There is a written policy on how to handle a violent co-worker or client.

___ There is a procedure to request the assistance of a co-worker.

___ There is a procedure to request the assistance of police.

___ I have received a verbal threat.

___ I have witnessed a threat of violence.

___ There is a procedure to deal with or report harassment.

___ I work alone.

___ No notification is given to anyone when I finish work.

___ There is an adequate alarm system.

___ There is adequate security in and out of building.

___ There is adequate security in the parking lot.

___ I have been assaulted by a co-worker.

___ I have witnessed incidents of violence between co-workers.

Please describe any of the above or additional unsafe work conditions that you have experienced.

____

Annexure B: Facility Security Risk Assessment Guidelines

Facility Security Risk Assessment Guidelines

Assessment Process Overview

The Risk Assessment process includes the following steps:

1. Identify the assets.
2. Determine the critical level of assets.
3. Identify the threats to each critical asset.
4. Identify the existing countermeasures (existing security is existing countermeasures).
5. Determine the vulnerability level of each critical asset.
6. Determine the risk level of each critical asset.
7. Recommend security upgrades to reduce high levels of risk.
8. Perform a cost-benefit analysis in support of upgrade recommendation if possible.

Definitions

Asset means a person, place, item, or information associated with the operation or function of the facility or organization. Its value may be quantifiable in terms of dollars. The total cost of damage to or loss of an asset is evaluated in the process. This may include replacement cost, repair cost, and the financial impact (consequence cost) of the loss event.

Loss event means physical or financial damage to or destruction of an asset. While human life is priceless, the process requires that each asset be given a value.

Critical level of an asset is determined by the impact its damage or loss will have on the continued operation of the business and its facilities and personnel. Criticality values are assigned on a scale of 1 through 4. See ***Rating the Impact of Loss*** section below.

Threat means any action or event, whether human or natural in origin, that can result in a loss event. Determine the probability of a specific threat successfully causing a loss event, not the probability of the threat occurring. This distinction is important and requires that the threats established be credible and realistic. A credible threat assessment and response should be established and is paramount to a successful security assessment. All possible threats, internal and external, must be carefully considered.

Countermeasure means any action or combination of actions involving physical, technical, administrative, procedural, or other measure(s) taken to reduce the severity of an identified risk.

Rating the Impact of Loss

The four levels of critical function(s) of an asset are as follows:
1—Essential: Total destruction of (or severe damage to) the asset would cause complete loss of business continuity. This is a catastrophic loss.
2—Critical: Total destruction of (or severe damage to) the asset would cause severe impairment of business continuity. This is a serious loss.
3—Important: Total destruction of (or severe damage to) the asset would cause noticeable impact on business continuity. This is a moderate loss.
4—Not important: Total destruction of (or severe damage to) the asset would cause no noticeable impact on business continuity. This is a minor loss.

Asset Vulnerability Rating
The level of vulnerability of an asset is determined by assessing the threats with the existing countermeasures. If the existing countermeasures are effectively protecting the asset from all threats, vulnerability will be low. If, however, the existing countermeasures are not adequate to prevent or withstand an attack, vulnerability is higher. Vulnerability is measured in terms of the probability of a loss event occurring. Vulnerability values are assigned on a scale of A through D. The levels of vulnerability are provided below.

Interpreting Probability of Loss
A—Extremely high: The magnitude of the vulnerability is such that if a threat occurs, there is an extremely high probability that it will be successful in causing a loss event.
B—High: The magnitude of the vulnerability is such that if a threat occurs, there is a high probability that it will be successful in causing a loss event.
C—Medium: The magnitude of the vulnerability is such that if a threat occurs, there is a medium probability that it will result in a loss event.
D—Low: The magnitude of the vulnerability is such that if a threat occurs, there is a low probability that it will result in a loss event.

Combine the criticality and vulnerability data associated with specific assets in such a way as to indicate the combined severity of impact and the probability of a loss event occurring. The criticality and vulnerability ratings assigned to the major assets are entered in a risk category chart to determine the overall risk probability rating as shown below.

Risk Categories

Asset Vulnerability and Criticality	**1 Essential**	**2 Critical**	**3 Important**	**4 Not Important**
(A) Extremely High	1A	2A	3A	4A
(B) High	1B	2B	3B	4B
(C) Medium	1C	2C	3C	4C
(D) Low	1D	2D	3D	4D

The risk assessment chart allows an employer to identify the most likely security risks with the highest potential severity in order to prioritize resources for security upgrades. This table indicates how the risk categories may be interpreted.

Risk Matrix Management Guide

Asset Risk Category	**Interpretation**
1A 1B 1C 2A 2B 3A	**These risks are very high and it is recommended that measures be taken to eliminate them.**
1D 2C 2D 3B 3C	These risks are moderate. Management may determine to address these risks.
3D 4A 4B 4C 4D	These risks are low.

Security Recommendations

Once the level of risk is determined for each asset, recommendations for security upgrades are made, if warranted. The first goal of the upgrades is to reduce the level of risk to those assets that are in the very high category to the greatest degree practicable.

A secondary goal is to reduce the level of risk to the assets in the moderate category to the greatest degree practicable. If there are constraints that preclude the immediate or near-term reduction of risks, recommendations should include planning and budgeting to accomplish this in the future.

When deciding which recommendations or countermeasures to use, the safety and security stakeholders for the organization need to discuss:

- Their immediate versus long-term needs;
- The feasibility of the addition or installation;
- The budget, including short- and long-term costs of the options; *and*
- How these will fit into the organizational climate and employee culture.

Risk Category	**Priority**
[Insert text]	

Jackson M. Katsigazi

Chief Executive Officer

Gold Circle
Investments
Limited