
Version History

| Version | Details of Amendment | Author | Date | Approver | Date |
|---------|---|--------|--------------------------------|----------|--------------------------------|
| 1.0 | Initial Document | CISO | 3 rd September 2018 | MD | 3 rd September 2018 |
| 1.1 | Addition to the scope of ISMS | CISO | 9 th January 2019 | MD | 9 th January 2019 |
| 2.0 | Annual Review and MIDC location Added | CISO | 13 th Nov 2019 | MD | 2 nd January 2020 |
| 3.0 | Annual Review and MIDC location removed | CISO | 2 nd Nov 2020 | MD | 10 th Nov 2020 |

SECURITY POLICY

To protect assets from all threats, whether internal or external, deliberate or accidental, CIPL will take measures to ensure that:

- *Information will be **protected against unauthorized access***
- ***Confidentiality** of Information will be assured*
- ***Integrity** of Information will be maintained*
- ***Availability of Information and Information Systems** will be met*
- ***Regulatory and Legislative** requirements will be met*
- ***Business Continuity** plans will be produced, maintained and tested*
- *Necessary **training** will be offered to maintain information security*
- ***Incident Management** process will be practiced to **keep damage to minimum** and to **prevent the recurrence** of the same*
- ***Internal policies and procedures** will be **reviewed periodically** for **continuous improvement***
- ***User Guidelines** stating **Do's and Don'ts** related to usage of internet, email, computer system, and measures taken for data protection will be established*
- *All employees, **Senior Management to L1 level employee**, will be **responsible** for **implementing and adhering to information security policies** within their scope of deliverables.*

Mr. Javed Tapia

Managing Director

SECURITY OBJECTIVES

| S. No. | Parameter | Objective | Periodicity | Responsible Team |
|--------|--|---|-------------|--------------------------|
| 1 | Average Minor Non-conformities per AUDIT Cycle (per department) | <=5 | 6 Monthly | ISMS |
| 2 | Internet Downtime (on Working days in working hours) | >=99% availability | Monthly | IT Team |
| 3 | Antivirus Pattern File Update | 98% | Monthly | IT Team |
| 4 | Overall High priority Incidence Occurrence Rate Admin +Facilities IT HR (should include incidents related to POSH) Customer Delivery/Project | <=5 <=5 <=5 | Monthly | Admin IT HR |
| 5 | Customer Satisfaction on Internal infrastructure | >=90% | 6 Monthly | Support/ Delivery/ IT |
| 6 | Repetition of Audit Findings in next Internal Audit | <=2 | 6 Monthly | ISMS |
| 7 | Count of residual risks | 90% | Yearly | ISMS |
| 8 | Full back up failures | <=2 times | Monthly | IT Team |
| 9 | Downtime due to power failure (during working hours) | <=6 hours | Monthly | Admin team |
| 10 | Number of employees relieved/ terminated without execution of HR Exit check list | =100% compliance | Quarterly | HR team |
| 11 | Background Verification for all employees | 100% | Monthly | HR Team |

Javed Tapia

Managing Director