# Information Technology and Information Security Governance Policy

AUTOMATIC SYSTEMS LTD

MARCH 2020

# Contents

# Digital information

## Purpose

The policy document combines legal requirements and current best practice for an information security management policy for the Company. It provides a policy with information security objectives, strategy and defines roles and responsibilities.

## Introduction

Information management is an essential part of good IT governance, which in turn is a cornerstone in corporate governance. An integral part of the IT governance is information security, in particular pertaining to personal information.

At ASL, we rely heavily on Information and Communication Technology (ICT) to conduct our business. We require ICT for our betting systems, for connectivity with our 24 outlets around the island, for our telephony systems, for all back office processes and for email communications etc. We have to ensure customers' satisfaction especially in this environment which is increasingly requesting connectivity that also helps in building the goodwill of the company. Effective IT Security Policy is of essence to the Company and part of the organisation's culture.

## Access to information

The Company has an Information Technology (IT) Policy identifying the rules and procedures for all individuals accessing and using the organisation's IT assets and resources. Users of the information system may only access those information system assets for which they have been explicitly authorized by the asset owner. Users may use the information system only for purposes for which they have been authorized, i.e. for which they have been granted access rights.

## Risk

We are subject to ICT risks such as Cyber Attack, Viruses and Malwares, Hardware and Software failures and Network disruptions. We are constantly on alert in order to mitigate those risks. As such, policies and procedures are in place to provide the security framework.

## Risk Management

The Board is responsible for overseeing information governance within the Company and ensures that performance of information and IT systems are adequate. An IT Risk Register is reviewed by the Audit and Risk Committee twice a year - or earlier if required, and a report made to the Board thereafter.

The Board and Management are involved in information and IT governance, such as:

- Oversee the realised total capital expenditures in line with budget at Board meetings;
- Regular evaluation of the information security systems; and
- Assess the need for independent evaluation from external experts on IT governance.

## Business Continuity

With our nature of operating being 24/7, business continuity is critical. We have Service Level Agreements (SLA) with international service providers, who have been chosen based on the quality of their systems as well as their ability to provide support within acceptable delays and set Recovery Time Objectives (RTO).

Our Websites are hosted by a well-reputed international hosting company and also hosted in-house, and are maintained by the said service providers and our dedicated IT team. We use industry standard security devices and software to mitigate cyber risks.

In addition, we promote awareness to our users of the inherent risks associated with digital information. User access rights are regularly reviewed. Our infrastructure consists of our primary site, running all our on-premise systems and applications and a Disaster Recovery (DR) site, where the most critical data are replicated in real-time and where backups are stored. Both our primary site and DR site are equipped with redundant Uninterruptible Power Supplies (UPS) and redundant power generators.

## Communication

For higher security control and business continuity, all communication connections with our outlets are centrally managed at our head office. The communication connection that is used for administration in outlets can also be used as a backup communication line in case there is failure in our critical communication lines. All our communication lines are secured using industry standard firewalls.

## Business alignment

In the constantly evolving technological environment, we do our utmost to keep pace with new technologies by evaluating their relevance in our industry and alignment with the business strategy. We are on the lookout for new technologies for running our business and also to improve our customers' satisfaction.

## Data protection

We collect, handle and store sensitive data in the course of our business. We do our utmost to protect this information and we are compliant with Mauritian Data Protection laws. A Data Protection Policy has been established as per The Data Protection Act 2017 and has been communicated to stakeholders. We regularly organize awareness programs with regard to data protection and privacy.