Optimal Workshop

Optimal Workshop

Technical and Organisational Security Measures

Date 8 November 2018
Version 1.0

1 INTRODUCTION

This document details the technical and organisational security measures that have been implemented by Optimal Workshop for the protection of customer provided information.

Optimal's security controls are based on the NIST 800-53A-R1 Standard security controls.

2 CURRENT MEASURES

The current organisational measures we have in place include, but are not limited to:

- Breach processes
- Business continuity plans
- Configuration management
- Disaster recovery measures
- Major Incident Response plan
- Management information and reporting
- Management of elevated privileges
- Regular assurance programme of third parties
- Regular penetration testing
- Regular security controls reviews
- Risk assessments
- Secure Coding and Application development guidelines
- Security awareness and training
- Security governance framework
- Security Policies and Standards
- Segregation of duties
- Staff vetting

The current technical measures we have in place include, but are not limited to:

- Anti-Malware measures
- Backups and data replication
- Building security
- Encryption at rest
- Encryption in transit
- Logging
- Monitoring and alerting

- Network segregation
- Platform hardening
- Replication of data
- Secure destruction of assets and data
- Shielding against DoS attacks
- Strong Access Control
- Vulnerability scanning of infrastructure, application code, and applications environment
- Use of AWS datacentres with strong security compliance
- Vulnerability and patch management