ACORA MANAGED SERVICE DESCRIPTIONS

The Choice of Leaders

SECURITY MANAGEMENT

CONTRACTED SERVICE HOURS

MANAGEMENT AND REPORTING	ACTION SECURITY INCIDENTS	MONITORING SECURITY INCIDENTS
Working Day - 08:45 – 17:30 GMT/BST	As per Incident Management Contracted Service Hours	24 hours' x 7 days per week x 365 days per year

SERVICE PURPOSE

To monitor the security of the Customer's Supported Environment for agreed types of security vulnerability, threats and compliance utilising Acora's standard systems and processes.

SERVICE SPECIFICS

Supported Environment	Specific IT/Services Supported Assets subject to Security Management
External Standards	Standards set by external sources against which Acora will measure compliance

SERVICE DESCRIPTION

- **Deployment:** Acora will deploy its Security Management Platform within the Supported Environment, which will monitor and report on relevant Security Incidents and provide ongoing security threat information to the Customer in relation to Vulnerability, Threat Detection and IT Compliance, as set out below.
- **Vulnerability Assessment**: Carry out continuous scans of pre-agreed critical items of the Supported Environment for security vulnerabilities and generate detailed reports listing threats by severity, which will be reviewed with the Customer on a monthly basis to discuss and agree actions to address or accept the risk that is presented.
- **Threat Detection:** Provide real-time security threat intelligence and threat prioritisation against the agreed items of Supported Assets to detect any malicious traffic within the Supported Environment. Acora will log serious Security Incidents with the Service Desk to action the threats in accordance with Incident Management.
- **IT Compliance Management:** Correlate security logs and Security Incidents from the Supported Environment into a single platform, which it will analyse on an ongoing basis to detect malicious behaviour. In addition, and where appropriate and agreed with the Customer in writing, Acora can assess compliance with relevant pre-defined external standards that form part of Acora's Security Management Platform.
- **External Standards:** The Pre-defined external standards available from Acora's Security Management Platform are a:
  - GLBA
  - HIPAA
  - ISO
  - NERC
  - PCI 2.0
  - PCI 3.0
  - PCI DSS 3.2
  - SOX

  The specific items from the above list that will apply to the Customer will be pre-agreed with Acora.

SECURITY MANAGEMENT REPORTS

For each month, a Security Management report will be provided to the Customer detailing:

- Number of security related alarms
- Summary of vulnerabilities detected and managed within the Supported Environment
- Compliance to external standards (where applicable against customer requirements using built-in reports)

Acora - Head Office
Acora House, Albert Drive, Burgess Hill, West Sussex, RH15 9TN T: +44 (0) 1444 232 000 W: acora.com E: enquiries@acora.com