ONECLICK FINANCIAL

Security Platform Features

- **24x7x365 Threat Detection and Response** – The Security Operations Center (SOC) monitors all security events and alarms 24x7x365. The SOC does triage and assessment of each event and escalates if the events are serious enough.

- **Security Analytics** – Utilizes a leading Security Information and Event Management (SIEM) platform paired with big data analytics platforms to collect and analyze data from the customer environment.

- **Host Protection** – Provides advanced host and network protection platforms targeted at zero-day and non-malware attacks, as well as traditional compromise tactics. Powered by a partnership with CrowdStrike. This data is fed into the SIEM and reviewed by the SOC daily.

- **Network Protection** – Using AlertLogic Threat Manager, this IDS monitors each network in the environment for network-based attacks and events of interest. This data is fed into the SIEM and reviewed by the SOC daily.

- **Vulnerability Management** – ChannelNet utilizes scanning and agent technologies to assess the customer's environment and uses this data to tailor the customer Security Operations Center's response to threats and attacks in the environment. This data is used to inform the SOC, which then works with the ChannelNet IT team to remediate any issues. Currently, we scan each environment weekly from an external perspective and monthly from an internal perspective. All scan results are reviewed by InfoSec. Remediation efforts are coordinated by InfoSec, if significant results are found.

- **Threat Intelligence** – The SOC consumes over 20 threat intelligence feeds, fusing the information together with internal data to respond to the changing threat landscape in real time. This data is correlated and cleansed based on reliability and applicability to the customer environment. It is used by the SOC to tailor protections and responses to alerts.

- **Distributed Denial of Service** (DDOS) protection is configured and monitored such that any large scale DDOS attack will trigger a mitigation to alleviate the impact of the attack on the web application/system. Any such occurrence requires the attention of both SOC engineers and InfoSec.

ONECLICK FINANCIAL

Hosted Environment Security

- **A formal IT risk management program** performs periodic risk assessments that identify critical assets, threats and vulnerabilities. This encompasses risk assessments of both the customer hosted environment and ChannelNet corporate environment. This also encompasses risk assessments of any new service, feature, tool that could potentially impact the security of ChannelNet or customer data.

- **Periodic firewall reviews** of customer hosted and ChannelNet environments with accompanying projects to mitigate any deficiencies or changes needed based on new threat/risk vectors.

- **Update / Maintain Information Security Policy** aligned with ISO 27001:2013.

- **Maintain segregation of duties** so that QA, Development and Production personnel only have access to the systems necessary to perform their individual function.

- **Maintain a mobile computing policy** that enforces company approved controls on any mobile device storing ChannelNet data.

- **Prevention of ChannelNet employees** auto-forwarding their email to external mail systems.

- **Maintain a remote access policy** that enforces company approved controls on any remote access to ChannelNet networks/systems.

- **Maintain an HR policy** that screens employees prior to employment, clearly defines security roles and responsibilities, ensures employees agree to all applicable policies and clearly defines termination or change of employment processes.

- **Implement and maintain a comprehensive security awareness** program that delivers security training and material to users on the newest or latest threats/trends in security. This includes new hire, periodic and annual training requirements.

- **Maintain an asset management** program that classifies all information and implements based on that classification.

- **Maintain processes to control/restrict access** to removable devices on ChannelNet computers.
- **Maintain a records management** process that retains information based on pre-defined periods.
- **Maintain strong access control mechanisms** across all ChannelNet systems, limiting user access on a least privilege model.
- **Maintain a privileged user account management process** that frequently rotates all privileged user account passwords.
- **Maintain an identity access management process** that controls the addition, modification and deletion of user or service accounts across all systems.
- **Maintain a password management process** that enforces highly complex passwords, two-factor preferred, for all systems.
- **Maintain an encryption/cryptography policy** that specifies the allowable encryption methods for all use cases / classifications.
- **Implement and maintain a strong physical security program** that limits access to various areas based on job function, which includes: limited badge access to data center(s), locked doors between public and reception and private areas, physical barriers from subfloor to super ceiling in all data centers, camera monitoring of all ingress/egress points, and a perimeter alarm system tied to security personnel.
- **Maintain a process to securely delete or destroy any sensitive information** on equipment needing to be reused or recycled.
- **Maintain a clear desk policy** that restricts users from leaving sensitive data lying around.
- **Maintain a change control process** that tracks and documents all changes to critical systems, with appropriate review and approval workflows.
- **Maintain processes that prevent production data** being used in non-production environments.

- **Maintain tools that protect ChannelNet systems** against malicious code.
- **Maintain a process to effectively back up critical systems.**
- **Maintain a central logging system** that stores security logs from all systems for at least one year.
- **Maintain a time synchronization process** that ensures all systems sync time from the same location.
- **Maintain a process to review all security logs daily** for critical security events.
- **Implement and maintain a process to identify new security vulnerabilities** across all systems along with programs to mitigate found issues.
- **Maintain a process to monitor wireless networks** for rogue access points or other wireless devices.
- **Maintain a process to assess any third-party relationships** for risk to ChannelNet or customer information/systems.
- **Maintain a secure development process** that performs static and dynamic code analysis for releases.
- **Maintain a process to manage third party service delivery**, ensuring security is as effective at the third party as if stored in house. This includes the addition of security language in all contracts with third party providers.
- **Maintain an incident response process** that organizes ChannelNet efforts in the event of a security incident.