TECHNICAL AND ORGANIZATIONAL MEASURES

INFORMATION SECURITY AND DATA PROTECTION

EFFECTIVE: JANUARY 6, 2020

1. **Protection of Information and Customer Data:**

ENGINE maintains administrative, physical, and technical safeguards for the security, confidentiality and integrity of information including Customer Data at a level not materially less protective than as described in this document and externally on our web site, as updated from time-to-time ("ENGINE Security Practices Page"). These safeguards will include measures for preventing unauthorized access, use, modification, deletion, and disclosure of Customer Data by ENGINE personnel. Before providing a third party service provider with logical access to Customer Data, ENGINE will ensure that the third party maintains at a minimum reasonable data practices for maintaining the security, confidentiality and integrity of the Customer Data, with such practices intended to prevent unauthorized access to or use of the Customer Data and not to be materially less protective that those set forth in the ENGINE Security Practices Page, as applicable to the services provided and proportionate to a level of risk as determined by ENGINE.

2. **Governance, Risk, and Compliance**
    a. ENGINE's information security program is aligned to ISO 27001, an international standard for security controls.
    b. ENGINE's Information Technology organization and related systems are certified for:
        i. ISO 27001, certificate # 586101
        ii. Cyber Essentials Plus, registration # QGCE1597
    c. ENGINE's Healthcare practice is certified for HITRUST CSF, account number HT-001985
    d. ENGINE is registered with the ICO, registration # Z2939946
    e. Formal risk assessments processes exist for both internal business units and our suppliers, thus ensuring a comprehensive and consistent approach to risk management. Risks are identified, recorded, classified, and treated as part of our ISO27001 management system.
    f. Our formal security program is resources and empowered through ENGINE's Executive Charter for Information Security and governed by an Information Security Oversight Board.
    g. Roles and Responsibilities for information security are defined in Engine's Information Security Management System.
    h. Engine's Chief Information Security Officer (CISO) is responsible security within the organization. Engine's CIO/Head of Information Technology is responsible for technology and security related Disaster Recovery and Business Continuity. Engine's Group Legal Counsel is responsible for Data Protection and compliance with legislation and regulations.
    i. ENGINE maintains an internal security audit function in the form of Compliance Assurance Plan (CAP) that has been developed to standardize a series of activities to measure and improve information security control effectiveness.

3. **Policies and Procedures**
    a. ENGINE information security policies and procedures are reviewed, updated, and approved by the Information Security Oversight Board and ENGINE's CISO on an annual basis.
    b. Information security policies and procedures are made available to staff upon

hire and ongoing as needed using an internal learning management system and through our corporate intranet.

c. Staff agree to adhere to policies as part of their contract of employment, with disciplinary procedures for non-compliance.
d. Operational procedures are documented whenever feasible to ensure a consistent and secure approach to processes.
e. Information security policy and procedures includes (but is not limited to) an Information Security Policy, Risk Assessment Policy and playbook, Clear Desk Clear and Screen Policy, Acceptable Use of Assets Policy, Data Classification and Handling Policy, Physical Security Policy, Incident Response Policy and playbook, Business Continuity Plan, and a Secure Asset Disposal Policy.

4. Physical and Environmental Security

a. ENGINE offices are closed workspaces and are sole occupancy.
b. Access control mechanisms such as key cards and numeric keypads are fitted to all ingress/egress points and secure internal locations.
c. Areas housing sensitive information or systems for the storage, transfer, or processing of data are restricted to ensure only authorized employees are permitted access.
d. CCTV systems exist in ENGINE offices including at all ingress and egress points; these retain video recordings for at least 30 days.
e. Visitors to ENGINE facilities must show valid identification, have an employee sponsor their visit, sign a visitor log, and wear a visitor identification badge.
f. ENGINE facilities are fitted with appropriate environmental controls for example fire extinguishing equipment.
g. Information processing equipment is architected for redundancy whenever technically and commercially feasible.
h. Primary information processing equipment is protected from power failures and other power anomalies.

5. Access Control and Identity Management

a. Security Assertion Markup Language through a common identity provider has been implemented on ENGINE systems wherever feasible to enable centralized access and session control and to provide single sign-on capabilities.
b. Multifactor authentication with a minimum of two factors is required for all ENGINE user accounts.
c. Password policy is compliant with the most current guidelines from the UK NCSC and NIST standard publication 800-53b.
d. Policy requires at least 12 characters and a combination of uppercase, lowercase, special characters, and numbers for all passwords.
e. Accounts are locked after consecutive invalid attempts.
f. A password policy enforcement tool is used to extend the default policy set in Microsoft Active Directory to include the following additional criteria:
    i. No common dictionary words
    ii. No character patterns
    iii. No passwords that include parts of the username
    iv. No previously breached passwords
g. Passwords are securely communicated and must be changed upon first logon.
h. System passwords are changed from their default passwords.
i. A user's identity must be validated prior to the IT team performing a password reset.
j. System administrators adhere to the tenet of least privilege and separation of duties; each are assigned with a standard and privileged account; both accounts are delegated minimum rights necessary for administrative and non-

administrative job functions.

k. Duties are segregated to prevent opportunities for collusion.
l. For non-system administrators, role-based access controls are used following the least privilege principle to ensure access is only permitted on a need to know basis.
m. User accounts are reviewed in accordance with ENGINE's Compliance Assurance Plan; this includes a review of inactive accounts, third-party (vendor /supplier) accounts, privileged accounts, service accounts, and authentication methods.
n. Access is terminated immediately following the reception of an employee termination notification.

6. Human Resources Security

a. Background and reference checks are conducted on all candidates for employment.
b. New employees must complete information security awareness training prior to being permitted access to ENGINE systems and on an ongoing basis, including monthly refresher training on focused topics and annual training on key topics such as e-mail security, data ownership, and shadow IT.
c. New employees must execute employment agreements, including confidentiality statements, prior to being permitted access to information systems.
d. Notifications are distributed to appropriate recipients on all changes in employment.

7. Security Operations

a. Accredited third-party penetration testing is conducted annually on externally facing systems.
b. Internal and external network vulnerability scans are conducted weekly by ENGINE's Information Security team.
c. Web-application vulnerability scans are conducted on a quarterly basis by ENGINE's Information Security team.
d. All vulnerabilities are managed in accordance with ENGINE's Vulnerability Management Policy and procedure; vulnerability remediation metrics are maintained to ensure process effectiveness.
e. An inventory of ENGINE assets including systems and associated data is maintained, and each asset is assigned an owner.
f. All IT assets and services are reviewed and approved by IT.
g. Build checklists are leveraged for the implementation of new information processing equipment to ensuring a hardened system configuration.
h. All changes must be submitted and approved in accordance with ENGINE's defined Change Management Policy and procedures prior to implementation.
i. Event logs recording user activities, exceptions, faults, and security events are produced, kept, and reviewed regularly.
j. Rules for the secure development of software and systems are established and applied.
k. A centralized logging utility is leveraged to enable the regular review and preservation of user activity and system logs.
l. Web and cloud application access, session control, and content filtering has been deployed to control access to online content and enable data loss prevention.
m. A device control utility is configured to prevent the use of unauthorized devices on user workstations.
n. Information security personnel are subscribed to various technical information security bulletins to proactively research and prevent threats that may impact the organization.
o. Various information security reports and threat intelligence are generated and

distributed to appropriate security personnel on a defined schedule.

p. Systems and network security appliances are constantly monitored for availability.
q. Security patching of all systems occurs on a regular basis as defined in ENGINE's systems maintenance procedures.

8. Data Protection

a. A defense in depth approach is leveraged by layering various administrative, physical, and technical controls to protect valuable assets.
b. Hardware firewalls exist at network perimeters and are configured to deny by default.
c. Intrusion Prevention Systems have been implemented to mitigate advanced persistent threats.
d. A centrally managed anti-virus and anti-malware solution has been implemented on ENGINE information systems including servers and workstations.
e. E-mail hygiene solutions have been implemented to mitigate attack vectors originating from e-mail messages.
f. A Data Loss Prevention system has been implemented to prevent sensitive data from being sent via email.
g. ENGINE leverages TLS 1.2 and AES-256 encryption wherever feasible to protect sensitive data in transit.
h. Data is logically segregated to ensure proper information containerization.
i. Backups of critical systems are scheduled daily, encrypted, and routinely tested.
j. Employee workstations including laptops are encrypted.
k. Production and non-production environments are segregated to ensure the proper segregation of duties for data access.
l. Production data is prohibited from being removed from production environments.
m. End of life equipment and media is disposed of by third-party providers who certify destruction of all data.
n. Retention and deletion of all data follows ENGINE's policies assuring client contractual, legal, and regulatory requirements for data disposal are followed.

9. Third Party Subcontractors

a. Vendors and suppliers that provide technology or data services undergo a third-party assessment to validate a standard level of security control implementation no less protective that ENGINE's own control measures.
b. Third party assessment reports are documented to communicate and track potential gaps to ensure acceptance and closure prior to use.
c. Third parties must undergo an accredited external penetration test, prior to use, to assure their environments are free from vulnerabilities.
d. Ongoing third-party due diligence activities are conducted to validate information security control effectiveness throughout the engagement lifecycle.
e. Requirements for information security are defined in third party contracts appropriate to the scope of work.

10. Business Continuity and Disaster Recovery

a. ENGINE's IT disaster recovery standard is based on ISO 27031, an internationally recognized standard for implementing a management system for business continuity with specific focus on Information and Communication technology (ICT) requirements. ISO 27013 follows a Plan, Do, Check, Act cycle for the management system and recovery processes.
b. Business Continuity and Disaster Recovery Plans have been established to ensure the quick and prioritized recovery of services following a disaster.

c. Business Continuity and Disaster Recovery Plans are tested in a live or table-top exercise at least annually.
d. ENGINE has adopted a rigorous technology standard and methodology based on redundancy and high availability, including:
    i. Redundancy and high availability by design throughout the IT infrastructure, eliminating single points of failure, especially for the core/central IT shared services and dependencies.
    ii. N+1 component redundancy in either active-passive or active-active configuration.
    iii. Geographically segregated facilities/computing locations.
    iv. Service provider and supplier diversity.
    v. Network pathway and carrier diversity.
    vi. Investing in and implementing technology platforms that are recognized as best-of-breed within their service areas, and which include robust feature sets suitable for high availability.
    vii. Adopting as part of overall IT strategy the following tactics:
        1. use of cloud services from best-of-breed providers that maintain their own robust standards for availability, assured by audit reports and backed by service level guarantees.
        2. use of private cloud and virtualization within ENGINE-managed solutions, including portability/replication of systems, platforms, data, and services as a required function.
        3. remote working –enabling the ability for staff to work and connect remotely at multiple entry points into the network and for online services.
e. ENGINE is a fully work-from-home capable organization and all staff are trained on effective work from home capabilities.
f. As part of its business continuity plan, ENGINE also maintains a dedicated Pandemic and Remote Working Plan; this plan was fully executed successfully during the 2020 Covid-19 outbreak.

11. Incident Response

a. An Incident Response Plan has been implemented to ensure a quick and orderly triage of information security weaknesses, events and incidents.
b. The Incident Response Plan is tested in a table-top exercise at least annually to ensure effectiveness.
c. A Security Incident Response Team charter with defined roles and responsibilities has been documented.
d. Staff are trained in the proper methods to report all identified and suspected information security weaknesses.
e. Multiple incident reporting channels are made available to staff.
f. Event logs are protected and retained to ensure proper audit trails during incident investigation and that such logs are tamper-proof.
g. A lesson-learned exercise must be performed following any actual incident response.