sales assessment .com

information systems security policy...

online sales talent assessment ←···

Approved: 2nd February 2010
Last updated: 2nd February 2010

···→

index...

···→ 1. Policy Statement

1. Policy Statement

1.1 Information is a critical asset of SalesAssessment.com Limited hereafter referred to as 'the Company'. Accurate, timely, relevant, and properly protected information is essential to the success of all the Company's activities. The Company is committed to ensuring all accesses to, uses of, and processing of Company and Customer information is performed in a secure manner.

1.2 SalesAssessment.com Limited is committed to working towards the adoption of a security model in line with BS7799/ISO27001 international best practice standards.

1.3 Technological Information Systems hereafter referred to as 'Information Systems' play a major role in supporting the day-to-day activities of the Company. These Information Systems include but are not limited to all Infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store Information owned by the Company or by its Customers.

1.4 The object of this Information Systems Security Policy and its supporting technical requirementspolicy is
to define the security controls necessary to safeguard Company Information Systems and ensure the security confidentiality and integrity of the information
held therein.

1.5 The Policy provides a framework in which security threats to Company Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of Information security controls throughout the Company

1.6 The Company recognises that failure to implement adequate Information security controls could potentially lead to:

- Financial loss
- Irretrievable loss of Important Company and Customer Data
- Damage to the reputation of the Company
- Legal consequences

Therefore measures must be in place, which will minimise the risk to the Company from unauthorised modification, destruction or disclosure of data, whether accidental or deliberate. This can only be achieved if all staff and partners observe the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and Company policies, and by adherence to approved Company Codes of Practice

1.7 The Information Systems Security Policy and supporting policies apply to all staff and partners of the Company and all other users authorised by the Company.

1.8 The Information Systems Security Policy and supporting policies do not form part of a formal contract of employment with the Company, but it is a condition of employment that employees will abide by the regulations and policies made by the Company from time to time. Likewise, the policies are an integral part of the Partner Agreements

1.9 The Information Systems Security Policy and supporting policies relate to use of:

- All Company networks connected to the Company Backbone

1. Policy Statement

- All Company-owned/leased/rented and on-loan facilities.
- To all private systems, owned/leased/rented/on-loan, when connected to the Company network directly, or indirectly.
- To all Company-owned/licensed data/programs, on Company and on private systems.
- To all data/programs provided to the Company by sponsors or external agencies.

1.10 The objectives of the Information Systems Security Policy and supporting policies are to:

- Ensure that information is created used and maintained in a secure environment.
- Ensure that all of the Company's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.
- Ensure that all users are aware of and fully comply with the Policy Statement and the relevant supporting policies and procedures.
- Ensure that all users are aware of and fully comply with the relevant UK and European Community legislation.
- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure all Company owned assets have an identified owner /administrator

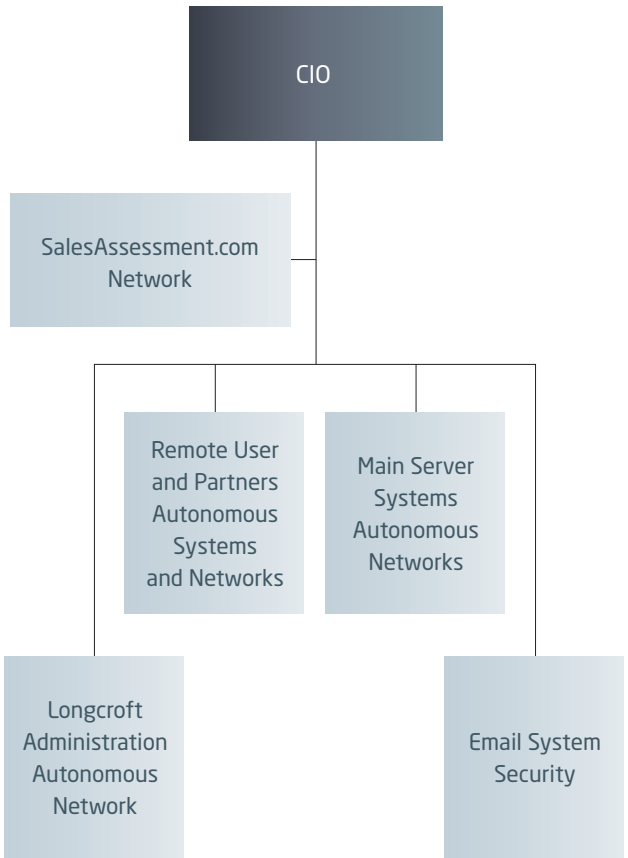
1.11 The Company Board has approved the Information Systems Security Policy and supporting technical policy. The Board has delegated the implementation of the Information Systems Security Policy, to the heads of each business and administrative areas. The CIO and his/her delegated agents will enforce the Information Systems Security Policy and associated supporting policy.

2. IT Security Governance

2.1 Security of the Company's IT and data assets cannot be achieved without a coherent governance model that ensures that all IT systems in Company are operated in accordance with approved policy and best practice.

The Company Governance model seeks to clearly define who is authorised to operate key IT systems and services and how individuals and groups wishing to operate new systems or services are approved and subsequently governed.

2.2 The Governance Model



2.3 CIO (Chief Information Officer)

The CIO is the governing body, responsible for the creation and annual renewal/review of the licences as well as the arbitration of disputes between the licensed bodies and the enforcement of all Company policies.

2.4 SalesAssessment.com network

This is the overarching name for all elements that comprise the Company network serving the staff, customer and partner population. This network is operated by Information Systems Services and provides central services and support to all users. The services of the main Company network are available to all users including users who are also members of other autonomously managed networks.

2.5 Autonomously Managed Networks

The autonomously managed networks (AMN's) are separate logical and physical networks created to address specific needs of a localised user population. They are operated under the control of the CIO and managed by outsourced, but suitably qualified staff. Each AMN appoints a named individual as the AMN manager this person is responsible for authorising requests locally and liaising with Information Systems Services.

2.6 Authorised IT Support Area Representatives

These individuals are nominated by each AMN as the person responsible for dealing with IT matters. These individuals may support specific applications and associated equipment.

···→ 2. IT Security Governance

2.7 Services to the Company Community

Only Information Systems Services and the defined autonomous networks may operate key central services including but not limited to Email, Internet Proxy, DNS, DHCP, Firewall, General Purpose Servers, Web Servers, Domain Services.

IT Support Representatives may operate specific applications and supporting servers which they should register with their AMN managers.

End users or individuals - who are not employed by AMN's or as IT Support representatives - who wish to run complex IT systems such as servers should first seek approval from their AMN management or apply to the CIO for AMN status if necessary.

2.8 The Network Perimeter

Information Systems Services acts as single point of contact for connections between Company Infrastructure and the Wide Area Network (including the Internet). Access through the network perimeter firewall is managed and operated by Information Systems Services.

Individuals located on the main Company network may make direct application for access through the firewall.

Individuals located in other AMN's should make application first to the authorised managers of their AMN who will approve the request and pass it on to Information Systems Services for final approval and action.

2.9 Communications

Good quality and frequent communications between all parties defined in this model are vital: The CIO reviews licences annually and communicates responses to all parties. Communications between Autonomous Networks is facilitated by a mailing list and bi-annual meetings hosted by Information Systems Services.

Communications between IT Support Area Representatives and Information Systems Services are facilitated by Mailing list and quarterly meetings hosted by Information Systems Services.

3. IT Management Roles and Responsibilities

3.1 The Company Board

The Company Board is responsible for approving the IT Security Policy, distributing the policy to all heads of departments/units/centres and for supporting the CIO in the enforcement of the policies where necessary.

3.2 The CIO

The CIO is responsible for annual review and approval of changes to the policy.

3.3 Heads of Business Areas

Heads of Business areas are required to familiarise themselves with the policies. Where a policy breach is highlighted heads of Business areas must co-operate in ensuring that appropriate action is taken. Heads of Business areas are obliged to ensure that all IT systems under their remit are formally administered either by an administrator appointed by the head of a Business areas or centrally by Information Systems Services. The duties of the administrator are set out in the associated supporting policy. (Security Policy).

3.4 Autonomous Networks

Where an area operates an autonomous network with a connection to the Company Backbone, then the respective Autonomous Network Manager is required to ensure that their operations comply with the IT Security Policy.

3.5 The CIO

The CIO is responsible for:

- Advising the Board, the Company officers, Administrators and other appropriate persons on compliance with this policy and its associated supporting policies and procedures.
- Reviewing and updating the Security policy and supporting policies and procedures.
- The promotion of the policy throughout Company.
- Periodical assessments of security controls as outlined in the Security Policy and supporting policies and procedures.
- Investigating Security Incidents as they arise.
- Maintaining Records of Security Incidents. These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed. The records will then be held in this anonymous format for a further two years for statistical purposes.
- Reporting to the Board, the Company officers, Administrators and other appropriate persons on the status of security controls within the Company.

3.6 Information Systems Users

It is the responsibility of each individual Information Systems user to ensure his/her understanding of and compliance with this Policy and the associated Codes of Practice.

All individuals are responsible for the security of Company Information Systems assigned to them. This includes but is not limited to infrastructure, networks, hardware and software. Users must ensure that any access to these assets, which they grant to others, is for Company use only, is not excessive and is maintained in an appropriate manner.

···→ 3. IT Management Roles and Responsibilities

3.7 Purchasing, Commissioning, Developing an Information System

All individuals who purchase, commission or develop an Information System for the Company are obliged to ensure that this system conforms to necessary security standards as defined in this Information Security Policy and supporting policies.

Individuals intending to collect, store or distribute data via an Information System must ensure that they conform to Company defined policies and all relevant legislation.

3.8 Third Parties

Before any third party users are permitted access to Company Information Systems, specific written approval from the CIO is required. Prior to being allowed to work with Company Information systems, satisfactory references from reliable sources should be obtained and verified for all third parties which includes but is not limited to; administrative staff, software support companies, engineers, cleaners, contract and temporary appointments. Data processing, service and maintenance contracts should contain an indemnity clause that offers cover in case of fraud or damage. Independent third-party review of the adequacy of and compliance with information system controls must be periodically obtained.

3.9 Reporting of Security Incidents

All suspected information security incidents must be reported as quickly as possible through theappropriate channels. All Company staff and partners have a duty to report information security violations and problems to the CIO on a timely basis so that prompt remedial action may be taken. The CIO will be responsible for setting up an Incident Management Team to deal with all incidents. Records describing all reported information security problems and violations will be created. These records will be encrypted and stored securely for six months after which time all information pertaining to individuals will be removed. The records will be held in this anonymous format for a further two years for statistical purposes.

3.10 Security Controls

All Company Information Systems are subject to the information security standards as outlined in this and related policy documents. No exceptions are permitted unless it can be demonstrated that the costs of using a standard exceed the benefits, or that use of a standard will clearly impede Company activities.

3.11 Compliance with Legislation

The Company has an obligation to abide by all UK legislation and relevant legislation of the European Community. The relevant acts, which apply in UK law to Information Systems Security, include but are not limited to:

- The Data Protection Act (1988/2002)
- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)
- Child Trafficking and Pornography Act (1998)
- Intellectual Property Miscellaneous Provisions Act (1998)
- Copyright and Related Rights Act (2000)

···→ 3. IT Management Roles and Responsibilities

- Health and Safety Act (1989)
- Non-Fatal Offences Against the Person Act (1997)
- Electronic Commerce Act (2000)
- ECommerce Directive (2000/31/EC)
- Regulations entitled European Communities (Directive 2000/31/EC) Regulations 2003 (S.I. No. 68 of 2003)

  The requirement for compliance devolves to all users as defined in (1.6) above, who may be held personally responsible for any breach of the legislation. Summaries of the legislation most relevant to the Company's IS policies may be found in the Guidelines accompanying the Policies. Full texts of the most relevant legislation are available from the Information Systems Services department and the Company CIO.

4. Breaches of Security

4.1 Monitoring

The Information Systems Services department will monitor network activity, reports from the Computer Emergency Response Team (CERT) and other security agencies and take action/make recommendations consistent with maintaining the security of Company information systems.

4.2 Incident Reporting

Any individual suspecting that there has been, or is likely to be, a breach of information systems security should inform the CIO immediately who will advise the Company on what action should be taken.

4.3 Enforcement

The CIO or his/her delegated agent has the authority to invoke the appropriate Company disciplinary procedures to protect the Company against breaches of security.

In the event of a suspected or actual breach of security, the CIO or his/her delegated agent may, after consultation with the relevant Administrator make inaccessible/remove any unsafe user accounts, data and/or programs on the system from the network.

4.4 Legal Implications

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the Data Protection Act 1987 and could lead to civil or criminal proceedings. It is vital, therefore, that users of the Company's Information. Systems must comply, not only with this policy, but also with the Company's Data Protection policy.

4.5 Disciplinary Procedures

Failure of a member of staff, or Partner, to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor to comply could lead to the cancellation of a contract.

5. Policy Awareness and Distribution

5.1 New Staff and Partners

This Policy Statement will be available from Information Systems Services on request. New staff and partners will be notified of the relevant policy documents when they initially request access to the Company network.

5.2 Existing Staff

Existing staff and partners of the Company, authorised third parties and contractors given access to the Company network will be advised of the existence of this policy statement. They will also be advised of the availability of the associated policies and procedures which are available on request.

5.3 Updates

Updates to Policies and procedures will be made periodically and will be posted to the IT Security web site.

5.4 Training

Training will be available from Information Systems Services in Information Security fundamentals on request.

6. Risk Assessment and Compliance

6.1 Risk Assessment

Risk assessments must be carried out periodically on the business value of the information users are handling and the information systems security controls currently in place. This is in order to take into account changes to operating systems, business requirements, and Company priorities, as well as relevant legislation and to revise their security arrangements accordingly.

6.2 Heads of Departments

Heads of Departments must establish effective contingency plans appropriate to the outcome of any risk assessment.

6.3 The CIO

The CIO will carry out risk assessments, review all risk assessments completed by other parties and highlight any measures needed to reduce risk in Information Security areas.

6.4 Internal Audit

The Company will carry out periodic Internal Audits to facilitate the assessment of risk management and compliance with the Information Security Policy.

6.5 Third Party Audit

Third Party Audits may be carried out at intervals, as deemed necessary by the Internal Auditor.

Supporting Policies amplifying this Policy Statement and Codes of Practice associated with these policies are published in an accompanying document and are available on request from IT Security.

Staff, partners and any third parties authorised to access the Company Network to use the systems and facilities as identified in paragraph 1.9 of this policy, are required to familiarise themselves with the policies and to work in accordance with them.

The supporting policies cover the general areas as listed below:

7. Supporting Policies, Review Documentation and Guidance Notes

- Network Security Policy
- Internet Use Policy
- Email Use Policy
- Password Policy
- Virus and Spam Policy
- Software Security Policy
- Data Backup Policy
- Disaster Recovery Policy
- Remote Access Policy
- Third Party Access Policy
- Incident Response and Misuse of IT Facilities Policy
- Legal Compliance Guidelines
- Technical Requirements Policy

sales assessment .com

online sales talent assessment

SALESASSESSMENT.COM LIMITED

AMERICAS

SalesAssessment.com Limited, 1800 JFK Boulevard,
Suite 300,Philadelphia, PA, 19103, USA

t: (888) 991-9891
e: inquiries@salesassessment.com
www.salesassessment.com

EMEA

SalesAssessment.com Limited, Longcroft,
Church Lane, Arborfield, RG2 9JA, UK

t: +44 (0)207 078 8818
e: enquiries@salesassessment.com
www.salesassessment.com

Brochure design by
Breathe Marketing Limited
www.breathe4u.com

version: 11.1