Dated 2nd February 2024

INFORMATION SECURITY POLICY

(incorporating GDPR)

INDEX

INFORMATION SECURITY POLICY

Elite Security Group inherently collects data during the routine course of business and such data may be retained for future reference or some other defined purpose. Data collection is typically relevant to employees, potential recruits, customers and/or suppliers, but additional data may be held relevant to a business function.

Elite Security Group has an ethical, legal and professional obligation to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability. We must ensure that the information we hold, or are responsible for, is safeguarded where necessary against inappropriate disclosure; is accurate, timely and attributable; and is available to those who should be able to access it.

This Information Security Policy provides the framework by which we take account of these principles. Its primary purpose is to enable all Employees to understand both their legal and ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.

This policy is the cornerstone of the Company's on-going commitment to enhance and clarify our information security procedures. It has my full support and I encourage all Employees to read it and abide by it in the course of their work.

Scott Huntley
Director of Support Services
2nd February 2024

INTRODUCTION

The current era is often referred to as the “information age”. We have seen a massive change in the way humans generate, store and exchange information. It has also profoundly altered the terms by which we interact with each other, not just as individuals, but also within and between institutions, societies and nations. We have accrued great benefits from this new era, but it brings with it profound challenges in the areas of security and privacy, which have been reflected in the growth of legislation around the globe concerning the holding of information.

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of the Company. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Elite Security Group to recover. This information security policy outlines Elite’s approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the organisations information systems.

Elite Security Group is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Company is responsible.

GDPR EXPLAINED

The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intended to strengthen and unify data protection for all individuals within the European Union (EU).

Fundamentally many of the concepts and principals are much the same as those in the previous Data Protection Act (DPA), so compliance does not necessarily start from scratch. The biggest change places a greater emphasis on the documentation that data controllers must keep to demonstrate their accountability.

Elite Security Group fully complies with the obligations set out in the **General Data Protection Regulations** (**GDPR**) and maintains records to that effect. Should you require further clarification as to the compliance of the organisation, please contact the Data Controller, Scott Huntley at our Head Office in Swindon.

INFORMATION CONFIDENTIALITY

The overriding premise is that any and all information sourced, created, used or retained by the Company is:

- used only for its intended purposes which are defined at the outset;
- retained only so far as is reasonable or necessary;
- used or communicated only so far as is required.

The highest ethical standards are required to prevent the inappropriate transfer or disclosure of sensitive information. The following list, whilst limited, provides an overview to the types of data the Company looks to retain as part of normal business operations. As previously identified, some of this information is required by law and/or some other justifiable reason. The Company is therefore keen to comply with GDPR whilst acknowledging its wider obligations where relevant.

Please note, this list is not exhaustive.

1) Personal Information of Employees
2) Training Records
3) Next of Kin Information
4) Work History of Employees
5) Credit Score of Employees
6) Payroll History
7) Court Orders (Attachment of Earnings Orders)
8) Client Information
9) Client Payment History
10) Client Property Information

INFORMATION ACCURACY

The Company will make every effort to maintain the accuracy of any data retained. In the event that such data becomes incorrect, or is otherwise found to require amendment, the Company will ensure this is done in a timely fashion, with amendments being recorded where appropriate, and incorrect data archived or removed as necessary.

The Company believes that the accuracy of data held for business purposes is not only a fundamental requirement of GDPR, but has a wider benefit to the business as a whole. It is in everybody's interest to ensure the Company works to maintain accurate, current and relevant information where appropriate.

INFORMATION CONSENT

The Company will always clarify the intended purpose of any data collection, where appropriate, and will limit the scope of any subsequent enquiries accordingly. Where Client information is sought, this will only be for the purposes of providing an agreed service provision and will not knowingly or intentionally extend beyond such parameters.

Elite Security Group sources information pertaining to individuals seeking employment in order to comply with the British Standard for Screening and Vetting (BS7858). This involves the use of a Credit Reference Agency, for the purposes of identity verification, and the Company adequately seeks permission for such a reference search to take place, in advance of one being carried out.

INFORMATION AVAILABILITY (INTERNAL)

Information is made available to individuals where appropriate, and where necessary for the ongoing performance of the business. There may be occasions where material is not made available and so the Company holds information in 3 notable levels of availability:

- site level;
- managerial level; and
- director level.

Site Level information will be limited to Assignment Instructions, Risk Assessments and other such material pertaining to their duties on site, or their ongoing employment with the Company. Managerial Level information may contain an overview of information including KPI performance data, Mobile Phone Directories, Fleet Management files, and other information which may be required for the ongoing performance of the business. Director Level information will include business strategy information, costing modules, and other highly confidential information not permitted for wider distribution.

INFORMATION AVAILABILITY (LAWFUL DISCLOSURE)

There are limited justifications for the disclosure of data without the consent of the subject to which the date pertains. For example, Article 6 (1) (c) provides such a justification whereby a disclosure is necessary for compliance of a legal obligation to which the Company is subject. There are other permissible justifications, and examples are:

1) Prevention of Terrorism Act (1989) and Terrorism Act (2000)

The Company MUST inform the Police if it is believed that information is available which may assist the authorities in preventing an act of terrorism, or help in apprehending or prosecuting a terrorist.

2) The Road Traffic Act (1988)

   The Company has a statutory duty to inform the Police, when asked, of any information that might identify any driver who is alleged to have committed an offence under the Act. It is not required to disclose clinical or other confidential information.

3) Court Order

   The Company may be required by Court Order to disclose information to an authority, regulator, or some other third party. In this regard, such disclosure is limited in its scope and is intended to comply with such an Order.

4) [*Some other enactment*]

   Some Acts of Parliament provide permission to disclose information but do not create a duty to do so. Often this is because of concerns that without a permissive power an organisation would be prevented from disclosing information even when it would be the 'right' thing to do. They are occasionally referenced by the Police when requesting information and so it is important to understand that where there is a choice about whether or not to disclose personal information to the Police, the requirements of both the Data Protection Act (1998) and the Common Law Duty of Confidentiality must be met. Where time permits you should seek advice from Scott Huntley, Director of Support Services.

INFORMATION MANAGEMENT

PAPER BASED SYSTEMS

Whilst the world moves towards paper-less systems, we ourselves are limited in this regard and so there will be occasions where data is retained or referred to in paper form. Naturally it is key to ensure that such data is only available for the purposes by which it has been retained, and not held on private (non-Company) premises. Furthermore, if this paper item cannot be scanned for long term retention (if appropriate or necessary), then sufficient effort must be made to ensure wider unauthorised access or distribution is limited or mitigated. Confidential paper-based data much be destroyed by either using the Company cross-shredder, or the approved waste disposal contractor 'Shred-It' for long term retention.

Whilst every effort is made to digitise records for long term retention, there is often a requirement to retain original documentation. It is the policy of the Company to store such paper-based records for a minimum of 8 years. In this instance, documents are suitably archived and identified with numerous “DO NOT DESTROY UNTIL *DATE*” labels. Boxes are then relocated to the Newbury Office storage facility and reviewed periodically. Such items will include Purchase Invoices, Payroll Data and Timesheets, HMRC and VAT Related Documentation. Where paper-based records are digitised, original records are destroyed in accordance with this policy.

Information should not be kept on desks for open view and so appropriate measures must be taken to ensure the protection of confidential information. This may include locking away materials overnight, or in secure office locations or cabinets. Care should be taken when printing confidential documentation as the communal printer may allow wider unauthorised disclosure. By extension, confidential material should not be left in vehicles unattended under any circumstances.

ELECTRONIC DATA SYSTEMS

Synchronised Server Facility

The server facility is very similar in concept to the widely known Dropbox product. However, we maintain some key differences. For example, each accessible folder can be limited by access level and editing or viewing functions. Some folders will therefore remain hidden to some users, and viewable only for others. This can be drilled down and expanded upon as necessary to ensure only the correct persons have access to the correct level of confidential information.

From a data integrity point of view; with 2048-bit RSA, SSL/TLS data encryption, data is replicated across multiple SSAE 16 type 2 certified datacentre locations with SAS RAID storage, maintaining an automatic failover with a 99.9% or better uptime SLA.

Importantly, the system maintains an audit trail of users including recording information on those who have accessed, amended, deleted or otherwise administrated any given document, whilst retaining versions and revisions - pre-amendments onwards. The system can also allow the administration of ‘read only’ sections where suitable, providing ultimate control over document storage and retention and dissemination.

DATA STORAGE

The Company employs a 'cloud' based system for data retention. With 2048-bit RSA, SSL/TLS data encryption, data is replicated across multiple SSAE 16 type 2 certified datacentre locations with SAS RAID storage, maintaining an automatic failover with a 99.9% or better uptime SLA.

The system maintains an audit trail of users including recording information on those who have accessed, amended, deleted or otherwise administrated any given document, whilst retaining versions and revisions - pre-amendments onwards. The system can also allow the administration of 'read only' sections where suitable, providing ultimate control over document storage and retention and dissemination.

DATA BREACHES

All computer systems and IT equipment are password protected to limit access to those machines often able to access data. Anti-virus is installed on every piece of equipment and backups are maintained through our standard of infrastructure.

In the unlikely event of a data breach the Company will investigate to understand the potential outcome of such a loss; for example, could such a loss result in the discrimination, damage to reputation, financial loss or loss of confidentiality of an individual. The Company would seek to address and remedy such a situation having sought Legal Counsel from the Company solicitors.

MANAGEMENT OF DATA BREACHES

In the unlikely event of a data breach the Company will investigate to understand the potential outcome of such a loss; for example, could such a loss result in the discrimination, damage to reputation, financial loss or loss of confidentiality of an individual. The Company would seek to address and remedy such a situation having sought Legal Counsel from the Company solicitors.

LAWFUL BASIS FOR PROCESSING DATA

The Company only requests or holds data specific to the intended function made clear at the outset. The Company does not hold data for marketing purposes, or for purposes which are manifestly different from which the original data was provided.

Whilst some data will be retained for the proper performance of agreed contractual obligations, as defined by Article 6 (1) (b) of the Regulations, much of the data retained is in compliance with some other parliamentary enactment or British Standards. For example; a) previous employment data may be retained to comply with the Screening and Vetting conditions of BS7858, a requirement of the Private Security Act 2001 b) pay information will be retained for the compliance of the Employment Rights Act 1996 and maintained for the ongoing performance of the business, and c) deductions from earnings will be recorded to comply with The Income Tax (Pay As You Earn) Regulations 2003.

The Company will only process data in compliance with the General Data Protection Regulation (GDPR). Where a potential risk or concern is identified, the Company will seek the advice of Legal Counsel before proceeding further.

PROTECTION OF INDIVIDUALS' RIGHTS

The Company fully complies with the rights of individuals in respect to the regulations and employs systems to adequately carry out the functions pertaining to an individual invoking such a right. Note: individuals have the following rights:

- The right to be informed;
- The right of access;
- The right of rectification;
- The right of erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- The right not to be subject to automated decision making (profiling).

SUBJECT ACCESS REQUESTS

All subject access requests are dealt with by the Director of Support Services, Scott Huntley. Unless compelled by subpoena, court order, legislation or some other enactment, such requests will be dealt with in accordance with the GDPR and will not usually be subject to charge. In the unlikely event of a refusal to comply with a subject access request, usually in the event of a manifestly unfounded or egregious request, the Company will identify the cause of resistance – with individuals retaining their right to complain the ICO.

Please Note: The Company has engaged the services of SAGE for the production of 'online pay slips' rendering simple 'subject access requests' potentially dealt with by way of individuals maintaining their own access points to this information. Furthermore, the Company will regularly review technologies and adapt accordingly to reduce any potential logistical implications of having to deal with regular requests.

RISK MANAGEMENT & MITIGATION

PAPER BASED SYSTEMS

1) Confidential material MUST NOT be left unattended or available for wider view
2) Confidential material MUST be stored in a lockable facility (where storage is necessary)
3) Confidential material MUST be used only for the identified intended purposes
4) Office desks MUST be kept clear of confidential data or material

COMPUTER BASED SYSTEMS

1) Computer systems MUST have basic Password Accessibility enabled
2) Computer systems MUST auto-install Windows and Microsoft Updates
3) Computer systems MUST maintain Norton Anti-Virus with Live Updates
4) All Company work product MUST be stored on the synchronised server facility

PROHIBITED PRACTICES

The following is a listed summary of unacceptable practices pertaining to data storage, data use or subsequent destruction of said data:

- Storage (for long term retention) on an unprotected USB
- Storage of confidential data on an unprotected USB
- Storage on the *Desktop* of a Computer
- Storage on any drive NOT known to be synchronised company wide
- Storage on any Backup Drive not subject to the company oversight

REMOTE ACCESS

Remote access (otherwise known as VPN) to the server as a file storage mechanism was disabled in 2016 in favour of the outsourced facility known as SYNC.

EMAIL USE

Emails and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. All emails must attach the standard company disclaimer at each footer, as prescribed by the Company from time to time.

Whilst the Company does not specifically prohibit the use of emails for personal use, it is worth noting that the Company email accounts may be monitored or accessed for the proper performance of business operations.

PERSONAL COMPUTER USAGE

The Company provided computer equipment for work use only. It is understood that there will be occasions when personal use may be required, but it is requested that this is kept to a minimum. Importantly, at no point should you download or install files or programs from any unknown source.

MONITORING OF SYSTEMS & FILES

The Company has the facility to monitor access to systems and electronic files and records, including monitoring any amendments or deletions made to these files. The Company will only use this ability to ensure the continued performance of business operations and prevent any act which may bring the Company into disrepute.

BUSINESS CONTINUITY PLAN

Elite Security Group maintains a separate Business Continuity Plan.

DATA CONTROLLER

Scott Huntley, Director of Support Services, is the nominated Data Controller and the Company is appropriately registered with the ICO. It is the intention of the Company to fully comply with best practice for the protection of data, whilst also employing reasonable and duly considered care and attention to the normal operations of the business.