#### 1. Introduction

This document sets out th Company name>> (the "Co protect data (electronic a Company, and to protect th computing environment, an Systems") from damage accidental.

For the purposes of this Poli

- a) <<insert list o
- b) <<add further

This Policy shall be subject Protection Legislation. "Date regulations in force from the privacy of electronic commuversion of the General Data as it forms part of the law of virtue of section 3 of the Eu Act 2018, the Privacy and E and any successor legislation

For the purposes of this Po Article 4 of the UK GDPR natural person (a "data sub identified, directly or indirec name, an identification num factors specific to the physi social identity of that natural

#### 2. Key Principles

- 2.1 All IT Systems and d
- 2.2 All IT Systems and Company Policies.
- 2.3 All personal data mu Legislation and the C
- 2.4 All employees of the the IT Systems and including, but not li "Users"), must ensur and comply with it at
- 2.5 All line managers m



n by all employees of <<insert ompany as a whole in order to , held, and processed by the systems, devices, infrastructure, vant equipment (collectively, "IT nternal, external, deliberate, or

e following type(s) of data:

in accordance with, the Data on" means all legislation and e use of personal data and the ot limited to, the retained EU law EU) 2016/679) (the "UK GDPR"), cotland, and Northern Ireland by al) Act 2018, the Data Protection s Regulations 2003 as amended,

all carry the meaning defined in g to an identified or identifiable tural person is one who can be rence to an identifier such as a nline identifier, or to one or more ic, mental, economic, cultural, or

gainst unauthorised access.

nly in compliance with relevant

pliance with the Data Protection n Policy.

all third parties authorised to use ind processed by the Company nd sub-contractors (collectively, th this Policy and must adhere to

under their control and direction

must adhere to and paragraph 2.4.

- 2.6 All data must be mar Data Protection Legi future in force.
- 2.7 All data must be clas data, "special catego GDPR), and confide system/procedure et appropriately in acco
- 2.8 All data, whether s available only to those
- 2.9 All data, whether s protected against un
- 2.10 All data, whether s protected against los
- 2.11 All IT Systems are upgraded by <<inser or by such third parauthorise.
- 2.12 The responsibility for stored thereon (inc confidentiality of that otherwise.
- 2.13 The responsibility for IT Systems lies with details>>] **AND/OR** responsible>>.]
- 2.14 All breaches of sec thereon shall be Department. [Any b personal data shall b and contact details>:
- 2.15 All breaches of secu shall be reported a Officer, <<insert nar individuals and/or de known or suspected Protection Officer, <<
- 2.16 All Users must repor or to the data stored concerns relate in a [instead] be reported
- 2.17 All Users must repor stored on the IT Sys name and contact and/or department(s) to personal data, su Data Protection Offic



at all times as required under

ance with all relevant parts of the cable laws whether now or in the

Iding, but not limited to, personal described in Article 9 of the UK eference to <<insert classifcation ata so classified must be handled ion.

r in hardcopy format, shall be need for access.

r in hardcopy format, shall be processing.

r in hardcopy format, shall be

tained, serviced, repaired, and partment>> (the "IT Department") partment may from time to time

ty of all IT Systems and the data to, the security, integrity, and partment unless expressly stated

y of data that is not stored on the ficer, <<insert name and contact individuals and/or department(s)

T Systems or any data stored lently investigated by the IT known or suspected to involve Protection Officer, <<insert name

t is not stored on the IT Systems igated by [the Data Protection **AND/OR** [<<insert details of the >>.] [Any breach which is either a shall be reported to the Data details>>.]

the IT Department. [If any such , such concerns must [also] **OR** officer.]

Data Protection Officer, <<insert insert details of the individuals such concerns relate in any way **OR** [instead] be reported to the

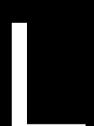
© Simply-docs – BS.DAT.SEC.01 Data Security

# 3. Department Responsibiliti

- 3.1 The IT Manager, <<i the following:
  - a) ensuring that compliance w
  - b) ensuring that implemented Company's s appropriate,] Company's s
  - c) ensuring that this Policy an rules whether the Data Prot
- 3.2 [The Data Protection [<<insert details of t be responsible for the protection of the protecti
  - a) ensuring that assessed and security requi
  - b) ensuring that effectively imp with the Company's see
  - c) ensuring that requirements and other rele but not limited
- 3.3 The IT Staff shall be
  - a) assisting all l aspects of thi
  - b) providing all matters and u
  - ensuring that are appropria responsibilitie
  - d) receiving and taking approp reports relate
  - e) taking proacti security proce
  - f) assisting the Company and any changes









letails>>, shall be responsible for

essed and deemed suitable for ty requirements;

thin the Company are effectively working in consultation with the nd Data Protection Officer, as come of such reviews to the

of the IT-related requirements of h, regulations, and other relevant orce including, but not limited to, e Computer Misuse Act 1990.

and contact details>>] **AND/OR** partment(s) responsible>>] shall

systems and methods are npliance with the Company's

within the Company are reviewed, working in consultation int [and Data Protection Officer, iome of such reviews to the

of the non-IT-related elated legislation, regulations, pr in the future in force including, Legislation.

ving:

nd complying with the IT-related

upport and training in IT security

vels of access to IT Systems that ng into account their job role, ity requirements;

ating to IT security matters and [including, in the event that any ng the Data Protection Officer];

e, to establish and implement IT areness;

tion to implement this Policy and future; and

- g) ensuring that Systems at i backups are backups shou
- 3.4 [The Data Protection [<<insert details of the be responsible for the second second
  - a) assisting all L related aspec
  - b) providing all l security matte
  - c) ensuring that appropriate for responsibilitie
  - d) receiving and matters and t event that an Protection Of
  - e) taking proacti security proce
  - f) assisting [<<i heads">>] AN security within implement thi future.

# 4. Users' Responsibilities

- 4.1 All Users must compusing the IT Systems
- 4.2 All Users must use t and must not use th likely to contravene a
- 4.3 Users must immedia Officer, <<insert namindividuals and/or de concerns relate to p security concerns rel
- 4.4 Users must immedi problems (including, which may occur on
- 4.5 Any and all delibera handled as appropria

#### 5. Software Security Measure

5.1 All software in use c systems, individual s and any and all i

© Simply-docs – BS.DAT.SEC.01 Data Security



en of all data stored within the IT <insert interval>> and that such ion [onsite] **AND/OR** [offsite]. All <insert type(s) of encryption>>].

nd contact details>>] **AND/OR** artment(s) responsible>>] shall

d complying with the non-IT-

pport and training in data

els of access to data that are account their job role, ty requirements;

hing non-IT-related data security in response [including, in the al data, informing the Data

e, to establish and implement areness; and

e managers" or "department on Officer] in monitoring data g all necessary action to s made to this Policy in the

s of this Policy at all times when

only within the bounds of UK law any purpose or activity which is or in the future in force.

ment and/or [the Data Protection AND/OR [<<insert details of the >>.] AND/OR [(and, where such rotection Officer)] of any and all r data.

partment of any other technical are failures and software errors)

s of this Policy by Users will be disciplinary procedures.

ling, but not limited to, operating firmware) will be kept up-to-date tes, patches, fixes, and other intermediate release Department. This pr 'major releases' (e.g particular major release software update is release, falling withir scope of this provisio

- 5.2 Where any security fixed immediately or such time as the sec affects, is likely to af Protection Officer sha
- 5.3 No Users may insta supplied on physical of the IT Manager. A IT Manager and may risk to the IT System agreements to which
- 5.4 All software will be ir an individual User is Such written permis and onto which comp

### 6. Anti-Virus Security Measu

- 6.1 Most IT Systems (in suitable anti-virus, fi such software will b definitions.
- 6.2 All IT Systems prote scan at least <<inser
- 6.3 All physical media ( Users for transferrin transferred. Such connection / insertio Manager].
- 6.4 Users shall be permi the approval of the I system must be scar
- 6.5 Any files being sent on physical media, scanned for viruses appropriate. [All ema
- 6.6 Where any virus is a the IT Department ( automatically fixes th and all necessary ac may involve the te Wherever possible a [immediately] **OR** [w

© Simply-docs – BS.DAT.SEC.01 Data Security









the sole discretion of the IT d to upgrading software to new ion 2.0), only to updates within a 0 to version 1.0.1 etc.). Unless a e it will be classed as a major are procurement and outside the

software that flaw will be either hdrawn from the IT Systems until ely remedied. [If the security flaw ffect any personal data, the Data ely.]

own, whether that software is ownloaded, without the approval Users must be approved by the that installation poses no security ion would not breach any licence bject.

ems by the IT Department unless on to do so by the IT Manager. which software may be installed by be installed.

d servers) will be protected with le internet security software. All the latest software updates and

re will be subject to a full system

s or disks of any kind) used by canned before any files may be performed [automatically upon ne User] **OR** [by the IT Staff /

cloud storage systems only with vnloaded from any cloud storage e download process.]

the Company, whether by email, shared cloud storage) must be part of the sending process, as ed automatically upon sending.]

must be reported immediately to en where the anti-virus software bartment shall promptly take any em. In limited circumstances this affected computer or device. mputer or device will be provided >>] to limit disruption to the User.

- 6.7 [If any virus or othe affect any personal o immediately to the D
- 6.8 Where any User deli IT Systems this will Act 1990 and will be procedures.

### 7. Hardware Security Measur

- 7.1 Wherever practical, securely locked whe in use or not (with au smart card, door cod Users must not allo reason.
- 7.2 All IT Systems not in to, servers, networ located, wherever po and/or in locked c members of the IT D
- 7.3 No Users shall have Users (including si permission of the l problem with such l reported to the IT De to rectify any such cases, instruction an
- 7.4 All non-mobile devi workstations, and physically secured i design of the hardw tampering with or the
- 7.5 All mobile devices smartphones) provie securely and handle are to be left unatten suitable container. L mobile devices from private homes or Col a vehicle it must be compartment.
- 7.6 The IT Department s All IT Systems shall the asset register.

# 8. Organisational Security

- 8.1 All Users handling da appropriately trained
- 8.2 All Users handling d

© Simply-docs – BS.DAT.SEC.01 Data Security



ely to affect, or is suspected to pove, the issue must be reported

malicious software or virus to the nce under the Computer Misuse under the Company's disciplinary

cated in rooms which may be priate cases, at all times whether anted access by means of a key, ess to such locations is restricted, cess to such locations for any

v Users (including, but not limited network infrastructure) shall be ecured, climate-controlled rooms accessed only by designated

is not intended for normal use by above) without the express nal circumstances, whenever a by a User, that problem must be imstances should a User attempt press permission (and, in most Manager.

limited to, desktop computers, ver possible and practical, be locking mechanism. Where the ases shall be locked to prevent

nited to, laptops, tablets, and should always be transported nces where such mobile devices ed inside a lockable case or other easonable efforts to avoid such at any location [other than their such mobile device is to be left in nd, where possible, in a locked

asset register of all IT Systems. responding data shall be kept on

sonal data) personal data will be

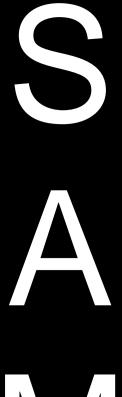
rsonal data) will be appropriately

supervised.

- 8.3 All Users handling da encouraged to exerc related matters that r
- 8.4 Methods of collecti personal data) shall
- 8.5 All personal [and no periodically, as set o
- 8.6 The performance of evaluated and reviev
- 8.7 All Users handling per principles of the Da Policies by contract.
- 8.8 No data, personal requires access to a have access to, su name(s) and/or posit
- 8.9 No data, personal or without the authorisa details>>.
- 8.10 All data must be h unattended or on vie

#### 9. Access Security

- 9.1 Access privileges for of Users' levels of au job roles. Users shal are not reasonably re
- 9.2 All IT Systems (and laptops, tablets, and or passcode, or such may deem appropri considered secure. O be used.
- 9.3 All passwords must,
  - a) be at least <<
  - b) contain a con spaces / syml
  - c) be changed a
  - d) be different fr
  - e) not be obviou dates, memor
  - f) be created by
- 9.4 Passwords should t should a User share











sonal data) shall be required and liscretion when discussing workter in the workplace or otherwise.

essing data (and in particular, d reviewed.

the Company shall be reviewed Retention Policy.

personal data shall be regularly

d to do so in accordance with the n and the applicable Company

hared informally and if a User erwise, that they do not already prmally requested from <<insert >>.

sferred to any unauthorised User and/or position(s) and contact

I times and should not be left or other parties at any time.

shall be determined on the basis any and the requirements of their to any IT Systems or data which of their job roles.

ces including, but not limited to, rotected with a secure password y-in system as the IT Department all forms of biometric log-in are roved by the IT Department may

puter, or device allows:

ers long;

lower case letters / numbers /

erval>> days;

d;

birthdays or other memorable laces etc.); and

User. Under no circumstances yone, including the IT Manager

© Simply-docs – BS.DAT.SEC.01 Data Security

and the IT Staff. No anyone at any time reason to believe th should change their of security to the IT I by an unauthorised in

- 9.5 If a User forgets thei The IT Department v to the IT Systems v which may be fully of for resolving the is immediately upon the
- 9.6 Users should not wri User cannot remem locked drawer or in a should passwords be to a computer display
- 9.7 All IT Systems with touchscreen etc.) s protected screensav inactivity. This time disable the screens disrupt any other processing).
- 9.8 All mobile devices smartphones) provid after <<insert time p other form of log-in period.
- 9.9 Users may not use the IT Systems with software must be rea job role and must b where such access r Data Protection Offic
- 9.10 [Users may connect tablets, and smartp appropriate>>] Com Department. Any ar Department governir Company network r devices shall be sut (including, but not lin the Company network pepartment shall res any such devices wit

#### 10. Data Storage Security

 All data stored in ele stored securely usin encryption.

© Simply-docs – BS.DAT.SEC.01 Data Security



ely asked for their password by hould be refused. If a User has s obtained their password, they and report the suspected breach personal data could be accessed ction Officer**11**.

e reported to the IT Department. eps to restore the User's access suing of a temporary password ember of the IT Staff responsible must be set up by the User the IT Systems.

b possible to remember them. If a ld be stored securely (e.g. in a ase) and under no circumstances s to see (e.g. by attaching a note

devices (e.g. mouse, keyboard, ere possible, with a password fter <<insert time period>> of ed by Users and Users may not screensaver will not interrupt or on the computer (e.g. data

nited to, laptops, tablets, and I be set to lock, sleep, or similar, uiring a password, passcode, or ar. Users may not alter this time

allow outside parties to access to of the IT Manager. Any such User for the performance of their eared by the IT Manager [and, cessible by the outside party, the

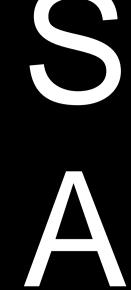
iding, but not limited to, laptops, rt specific network name(s), if ect to the approval of the IT equirements provided by the IT i devices when connected to the times. Users' use of their own y, all relevant Company Policies those devices are connected to art of the IT Systems. The IT t the immediate disconnection of

rticular personal data, should be ert type(s) of encryption>>] data

- 10.2 All data stored in h media, and in partice box, drawer, cabinet,
- 10.3 No personal data sh limited to, laptops, ta the Company or oth Protection Officer ar with all instructions a and for no longer tha
- 10.4 No data, and in p computer or device p is a contractor or su User has agreed to and the Data Protect

### 11. Data Protection

- 11.1 All personal data concentration collected, held, and Data Protection Leg and the Company's I
- 11.2 All Users handling d and must comply wit at all times. In particu
  - a) All emails co Policy must b
  - b) All emails con Policy must b
  - c) Personal dat transmitted o networks is not
  - d) Personal data transmitted or reasonably pr
  - e) Personal data body of an el from the bod should be del be deleted [u
  - f) All personal transferred p shall be trans
  - g) Where any p
    being viewed
    be left unatte
    computer and
- 11.3 Any questions relati Protection Officer,] <











ronically on removable physical d be stored securely in a locked

mobile device (including, but not , whether such device belongs to nal written approval of the Data approval, strictly in accordance at the time the approval is given, /1.

should be transferred to any User unless the User in question behalf of the Company and that pmpany's Data Protection Policy

essed by the Company will be ordance with the principles of the f the Data Protection Legislation

he Company shall be subject to, ompany's Data Protection Policy ply:

nd/or other data covered by this ert type(s) of encryption>>];

nd/or other data covered by this

overed by this Policy may be ly; transmission over unsecured rcumstances;

ered by this Policy may not be there is a wired alternative that is

ed by this Policy contained in the ceived, should be copied directly tored securely. The email itself associated therewith should also teletion>>];

on removable electronic media, iner marked "confidential".

er data covered by this Policy is nd the computer in question is to f time, the User must lock the

hould be referred to [the Data t details>>.

© Simply-docs – BS.DAT.SEC.01 Data Security

#### 12. Deletion and Disposal of Data

- 12.1 When any data, and disposed of for any r no longer needed), it <<insert method(s)>
- 12.2 For further informatic refer to the Company

#### 13. Internet and Email Use

- 13.1 All Users shall be s Company's Commun Systems.
- 13.2 Where provisions in ensure security wh requirements impos Users must take suc

### 14. Reporting Security Breach

- 14.1 Subject to paragrap known breaches that [<<insert specific na [a member of the IT]</li>
- 14.2 Subject to paragrap known breaches tha referred immediately Officer] AND/OR [< responsible>>].
- 14.3 All concerns, questic personal data shall Officer] OR [<<ins responsible>>] who Data Protection Polic
- 14.4 Upon receiving a department respons including, but not lin take any and all such
- 14.5 Under no circumstan their own without firs Data Protection Offic security breaches un the <<insert details c appropriate.
- 14.6 All security breaches

#### 15. Policy Review

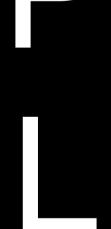
The Company shall review t as required in order to en

© Simply-docs – BS.DAT.SEC.01 Data Security











a, is to be erased or otherwise opies have been made and are d and/or disposed of using

posal of personal data, please

mply with, the provisions of the ernet Policy when using the IT

additional steps to be taken to or email over and above the ons, Email and Internet Policy,

estions, suspected breaches, or s shall be referred immediately to tment] **OR** [the IT Manager] **OR** 

estions, suspected breaches, or covered by this Policy shall be me>>] **OR** [The Data Protection ndividuals and/or department(s)

, or known breaches that involve ly to the [The Data Protection ividual(s) and/or department(s) accordance with the Company's

of a breach, the individual or ert period>>, assess the issue associated therewith, and shall ry to respond to the issue.

ot to resolve a security breach on individual or department [(or the ers may only attempt to resolve d with the express permission of, department(s) responsible>>, as

hall be fully documented.

<<insert interval>> and otherwise -to-date and fit for purpose. All questions, concerns, and communicated to the <<ir responsible>>, as appropria and contact details>>].



ng to this Policy should be lividual(s) and/or department(s) rotection Officer, <<insert name

rt date>>. No part of this Policy y to matters occurring on or after

#### 16. Implementation of Policy

This Policy shall be deeme shall have retroactive effect this date.

This Policy has been approv

Name: <<	<insert< th=""></insert<>
----------	---------------------------

<<insert |

<<insert of

Position:

Date:

.....

**Due for Review** <<insert of by:

Signature: