

Group Standard

Acceptable Use of Information Systems



Serco recognises its responsibility to ensure that employees access, process and publish information in accordance with Serco's social and ethical principles, legal requirements, with appropriate privacy and security, and in a manner that maintains and enhances the reputation of the company

Document Details

Document Details	Serco Business
Reference SMS GS-BC1	Version 5
Approval Date July 2017	Date for next review July 2019
Applicability Serco Group covering all business regions, operating companies and business units throughout the world ¹ covering: <ul style="list-style-type: none"> - employees, officers, directors and individuals working as consultants and contractors and any other parties acting as representatives or agents of Serco (Employees) - wholly owned subsidiaries and majority-owned operations Where a minority interest and in regard to its subcontractors and suppliers Serco encourages alignment with this Standard	
Authority Chief Executive, Serco Group plc	
Accountable Policy Owner (Group) Chief Information Officer	
Additional Information Supporting standards, standard operating procedures and guidance relating to this Group Standard are available within the Serco Management System	
Governance Our policies and standards, together with any regional or market requirements and enhancements to them, are authorised through a robust governance process.	
Consequence Management As a Group Standard the requirements detailed in this document are mandated and must be adhered to. Non-compliance will have consequences which may include disciplinary action. The Consequence Management Group Standard (SMS-GS-G1) details how instances of non-compliance will be dealt with	
<small>¹As used herein, Serco Group and its affiliates, subsidiaries and operating companies are referred to as "Serco". The "Company" or "company", or "we", "us" or "our"</small>	

Contents

1	Objectives.....	2
2	Policy Standards.....	2
2.1	General requirements.....	2
2.2	Training and awareness.....	3
2.3	General principles and personal use.....	3
2.4	Internet.....	3
2.5	Electronic publishing – use of social media.....	3
2.6	Intranet.....	4
2.7	Electronic mail and messaging.....	4
2.8	Keeping information secure.....	5
2.9	Monitoring.....	7
3	Responsibilities & Accountabilities.....	7
4	Processes and Controls.....	9
4.1	Governance processes and controls.....	9
4.2	Key processes and controls.....	13
5	Supporting documentation and guidance.....	15
6	Definitions.....	15
7	Further information and support.....	16

1 Objectives

Serco recognises its responsibility to ensure that employees access, process and publish information in accordance with Serco's social and ethical principles, legal requirements, with appropriate privacy and security, and in a manner that maintains and enhances the reputation of the company.

This standard sets out the behaviours that are required to be adopted, the rules that employees must abide by and the legal requirements that must be complied with when using information systems, which includes the internet, social media and email (whether or not they are provided by Serco and whether or not they are used in or outside of work) to access, process and publish information either owned by or referencing Serco, our employees, clients or business partners.

All media should be assumed to be open to public scrutiny and individuals have a responsibility to consider any materials they publish or write in the light of public opinion. Individuals and managers need to be mindful that, as a private company, Serco is even more susceptible to public view and opinion than other organisations and should therefore be especially vigilant.

2 Policy Standards

2.1 General requirements

- S1. Serco fully respects the legal rights of our employees in all countries in which we operate. However, activities which affect Serco's business interests (whether in or outside of work) are a proper focus for company policy.
- S2. All employees will ensure that their actions and the information they access, process and publish which relate to Serco (whether in or outside of work) comply with:
 - a. Serco's values
 - b. Serco's Code of Conduct
 - c. relevant Serco policy standards and operating procedures
 - d. all applicable laws (including copyright, trademarks, the fair use of material owned by others and data protection legislation), and
 - e. do not result in harm or damage to Serco's reputation
- S3. The loss of any device such as laptops, tablets, mobile phones, PDAs, removable media devices (i.e. USB stick, CD, memory card etc.), document or any paperwork that contains information with a Protective Marking or marked as 'Serco Restricted and Sensitive', will be reported as a security incident, in line with the Security Group Standard¹
- S4. Contracts, customers, Business Units or Divisions may have additional requirements for acceptable use over and above those detailed in this standard. Any additional requirements for the acceptable use of information systems which are applicable to your job and/or place of work must be read and understood
- S5. Failure to comply with these requirements for acceptable use, may lead to disciplinary action and/or legal proceedings. Failure to comply may also result in legal proceedings against Serco

¹ See Security Group Standard Ref: SMS-GS-S1

2.2 Training and awareness

- S6. New employees will be advised, and existing employees regularly reminded, of the Company's policies and requirements in regard to the acceptable use of information systems and will be provided with updates to those policies or changes in local requirements

2.3 General principles and personal use

- S7. Information systems (IS) provided by Serco may be used for appropriate personal use. However, personal use should only ever be of a reasonable duration and frequency, and must not detract from your performance or that of your colleagues, harm the company's reputation or interfere with the operation of Serco's business
- S8. Telephones (including mobile phones and Personal Data Assistants (PDAs) provided by Serco) may be used to make a reasonable level of personal calls.
- S9. Telephones provided by Serco will not be used to make calls or send texts to premium rate numbers (unless specifically required to do so for business reasons), access non-business related subscription services or applications, or make private international calls (except when abroad on company business)
- S10. No calls made or texts sent will be abusive to or harass the recipient
- S11. Serco's information systems will not be used to conduct any unapproved private employment or business activities that are not related to Serco's business
- S12. Serco may monitor your use of the internet, email, messaging and other information systems for security and compliance purposes
- S13. The use of IS will comply with all applicable laws of the country/territory in which the use takes place.
- S14. Serco may limit the personal use of IS where the company considers this is appropriate due to possible or actual interference with its business
- S15. Employees who are issued with a standard Serco PC will only rebuild or change any configuration with the permission of their IS support team

- S16. An employee must not copy any commercially sensitive, confidential or privileged information belonging to Serco, our customers or third party partners to any personally owned computers or devices except those enrolled in an approved BYOD programme which is covered by a separate personal contract with the employee

2.4 Internet

- S17. IS provided by Serco will not be used to:
- view, create, amend, distribute, transfer, store or print information that is pornographic, obscene, indecent, hateful, defamatory or offensive
 - engage in any form of illegal activity, including fraud, plagiarism, forgery, any form of intimidation or harassment
 - participate in online gambling, or for soliciting for personal gain or profit
 - download, store, copy or transmit the works of others (including software, games, music and video files), without their permission, where this infringes copyright or otherwise contravenes the owner or licensor's terms and conditions regarding permitted use

All information created will be fair to and respect all religions, political, economic and racial differences and opinions and show proper consideration for others' privacy

- S18. Employees will not commit Serco to any form of contract or obligation or enter into any IS third party contract (e.g., internet-based services, Software as a Service (SaaS) or applications) without appropriate authorisation
- S19. The use of the internet, including social media must not affect the work employees are required to perform for Serco. Should this be the case, then the company may decide to limit access to the internet and other IS for personal use

2.5 Electronic publishing – use of social media

- S20. In general, Serco recognises the rights of our employees to use social media as a medium of self-expression

- S21. Material which refers to Serco or uses the company's name on multi-media and social networking websites (such as MySpace, Facebook, YouTube, Bebo, LinkedIn, Twitter, blogs, wikis, newsgroups and any other site where text can be posted) may be published, providing that this is done in a professional and responsible manner and does not harm or tarnish the image, reputation and goodwill of Serco and our employees in a knowingly or recklessly defamatory manner
- S22. Information that is false or otherwise defamatory about an individual or organisation directly connected to Serco (for example, Serco employee, customer, supplier or partner) shall not be published
- S23. Any information that is published must be correct and fair, and where mistakes occur, must be corrected in a timely manner
- S24. When publishing information related to work or subjects associated with or about Serco in a personal capacity, it must be made clear that the comments and views expressed are personal and do not represent those of Serco; a disclaimer on such comments will be used, e.g. "The postings on this site are my own and don't necessarily represent Serco's positions, strategies or opinions." Personal views or opinions must not harm the company's image and reputation
- S25. Information will not be published which could compromise personal security of colleagues, customers or the business. Particular care will be taken regarding government or public sector clients. Employee vetting status or the sensitivity of the work done will not be disclosed
- S26. Information that is confidential or proprietary to Serco or to any third party that has disclosed information to Serco will not be published or used
- S27. All requests from the company not to discuss topics for confidentiality or legal reasons will be complied with. Similarly, requests made by Serco to remove information which has been published which breaches legislation, regulations or company policies will be complied with
- S28. Material will be kept up-to-date and care taken not to compromise Serco intellectual property, misrepresent Serco or communicate in a manner which may harm the image and reputation of the company

- S29. If material is found on-line about Serco that is wrong, unfair, or potentially defamatory, this will be notified to line management or the Divisional communications team

2.6 Intranet

- S30. Information available on Serco Group's intranet (known as Our World, The Hub and other collaboration systems), is intended solely for use by Serco. Third parties will only be permitted access to the information on the intranet where a confidentiality agreement is in place, and where there is a legitimate Serco business requirement for the third party to have access, (which will be limited to the specific information needed to fulfil the business requirement)
- S31. Only information relating to Serco business will be published on its intranet, and this must clearly indicate the appropriate classification, as detailed in the Information Privacy Classification Operating Procedure²

2.7 Electronic mail and messaging

- S32. All employees are responsible for the content of all text, audio and images that they send using Serco's electronic mail (email) and other messaging systems (which include instant messaging and text messaging)
- S33. Material that is pornographic, obscene, hateful or defamatory, or that is intended to harass or intimidate any other individual will not be sent or solicited using Serco's information systems
- S34. If such material is received it must be reported to line management. The email should be retained in your inbox until advised of the appropriate course of action that should be taken
- S35. Only email addresses and messaging systems supplied by Serco, our customers or partners will be used to send and receive information related to any business conducted on behalf of the Group
- S36. Personal email accounts (e.g. Hotmail, Yahoo, Gmail), instant messaging and text messaging systems will not be used to transfer information with Protective Marking, sensitive information owned by or relating to

² See Information Privacy Classification GSOP Ref: SMS GSOP S1-5

customers, or marked 'Serco Restricted and Sensitive' or 'Serco Business', as these are not as secure as Serco's email systems

- S37. Serco's standard disclaimer, which is attached to the end of each email sent from Serco's email systems, must not be removed
- S38. Email and messaging systems will not be used to generate unsolicited messages, including the sending of junk mail or other advertising material to individuals who have not specifically requested such material
- S39. Spam email and messages will not be replied to or forwarded to any other individual, as they often contain malicious content or harmful links
- S40. Anonymous emails will not be sent from Serco systems, nor will email and messaging systems be used to create or forward 'chain letters', 'Ponzi' or other 'pyramid' schemes of any type
- S41. Vigilance should be maintained for suspicious looking email and messages, which should be deleted immediately, and the local IT department or manager informed. In case of any subsequent forensic examination the suspicious email must be retained in the deleted or recovery folder for a minimum of one month
- S42. The content of email and messaging systems provided by Serco is subject to the Group standards and procedures regarding business records retention, storage and deletion³

2.8 Keeping information secure

2.8.1 Passwords

- S43. All passwords assigned for the use of Serco information systems will be kept safe. User identity or passwords or any other access code must not be written down, displayed or disclosed to any other individual. Users must not access information with a user identity or password which is not their own
- S44. If an employee has any suspicion that their password has been used by some other person, then they must change their password and report it as a security incident, in line with company procedure⁴

- S45. Passwords will be created and managed in accordance with Serco's password guidelines, the key requirements of which are:
 - a. passwords will be a minimum of 8 characters in length, consisting of upper and lowercase letters and numbers. The password will be changed at least every 90 days
 - b. when changing passwords, those that have been used in the previous 13 months will not be re-used
 - c. passwords that could easily be guessed by others (i.e. birthday, children's names etc.) will not be used
- S46. If there is a legitimate reason to provide a password to the IT department, then it will be changed immediately on completion of the support activity
- S47. The digitised signature of another will not be used or stored without their consent

2.8.2 Privacy

- S48. All information will be classified in accordance with the Group Security Standard⁵
- S49. It is the responsibility of the employee to ensure that their laptop is encrypted in line with company policy
- S50. Information with protective marking or classified as 'Serco Restricted and Sensitive' will not ordinarily be copied onto removable media, unless there is a significant and unavoidable business requirement to do so. If this information needs to be stored on USB flash drives, the device used will be approved by Serco and provided with built-in encryption
- S51. Similarly, information held on other types of removable media will be encrypted using Serco approved encryption software
- S52. Information with a protective marking or marked 'Serco Restricted and Sensitive' will be encrypted when transmitted by electronic means (email or file transfer) over the internet
- S53. Information with a protective marking, or marked as 'Serco Restricted and Sensitive' will not be disclosed to any person who does not have the right or need to know

³ See Document Retention GSOP Ref: SMS GSOP III1-2

⁴ See Incident Reporting and Management GSOP Ref: SMS GSOP O1-2

⁵ See Security Group Standard Ref: SMS-GS-S1

- S54. Sharing of the information with a marking of 'Serco Restricted and Sensitive' or 'Serco Business' with third parties requires the completion of a Non-Disclosure Agreement (NDA) with the third party prior to sharing
- S55. Personal information will only be held or processed in accordance with relevant national and territory law. Unauthorised information about Serco employees will not be provided or disseminated to outside parties
- S56. Personal computers (desktop and laptop) will be locked (using the Ctrl+Alt+ Delete then Lock Computer or by activating the Sleep or Screen Saver options on Apple PCs), and documents with a Protective Marking, or marked as 'Serco Restricted and Sensitive' secured when left unattended, to prevent unauthorised access
- S57. Desktop and laptop computers will be powered down when in transit or when not in use for a significant period of time, as encryption is not enabled and the confidentiality of information compromised if the machine is placed in sleep or standby modes
- 2.8.3 Information Systems**
- S58. When transported in a vehicle, PCs and other IS equipment will be stored in the boot. PCs and other IS equipment will be stored in the boot when a vehicle is unattended, and the vehicle must be locked. For IS equipment holding any form of sensitive information an assessment must be undertaken with the local security lead as to whether a vehicle boot safe is required. PCs and other IS equipment will not be left in the vehicle if unattended for a longer period of time (i.e. overnight)
- S59. IS equipment will not be left unattended in a public location (including airports, hotel lobbies, train stations, internet cafes, etc.) or on public transport, taxis, trains and planes
- S60. IS equipment will not be connected to Serco or customer-owned communication networks without permission from Serco and the relevant network owner
- S61. Anti-virus software, including a subscription to an update service, must be installed on any device which is used to connect to Serco, customer or third party networks and information systems
- S62. An appropriate and approved method of encryption will be deployed to prevent unauthorised access to Serco Restricted and Sensitive information held on PCs (desktop and laptop), portable devices and removable media, and when transmitted using email and other electronic file transfer systems to any third parties
- S63. All Serco PCs/devices and removable media used for business purposes will have an appropriate and approved method of encryption and corporate device management, unless permanently located wholly within secure Serco premises or if the site has been approved by the Divisional Security Lead as being secure
- S64. Any non-Serco PC/device or removable media that is used to store Serco Business, Serco Restricted and Sensitive or customer data will have an approved method of encryption and corporate device management, unless permanently located wholly within secure Serco premises or if the site has been approved by the Divisional Security Lead as being secure. This includes employees' personal PC/devices whether or not they are part of a Bring Your Own Device (BYOD) programme or equivalent and any PC/devices used by suppliers, consultants or contractors
- S65. Malicious programmes (e.g. viruses, trojans, email bombs etc.) will not be intentionally introduced into Serco's, our partners' or our customers' information systems, unless specifically authorised to do so as part of approved security activities
- S66. No employee will:
- disrupt network communications, interfere with, harass or deny service to any other user or make changes to another IS system that renders it unusable by others
 - intentionally access or transmit information about, or software designed for, breaching security controls
 - create computer viruses or monitor or intercept network traffic, unless specifically authorised to do so as part of security activities
 - remove or disable company-installed anti-virus software and malware controls
 - attempt to crack or capture passwords or decode encrypted information

2.9 Monitoring

- S67. Serco is ultimately responsible for all business communications but will, as far as possible and appropriate respect the privacy of our employees whilst working
- S68. Serco has the right to monitor the communications and use of Serco's information systems by our employees, in order to:
- ensure that standards are adhered to
 - prevent unauthorised use
 - comply with legal obligations
 - prevent and detect criminal activities
 - ensure secure and effective operation
- S69. The company may review content stored on its information systems and monitor telephone, email and internet traffic data (i.e. sender, receiver, subject, attachments to emails, numbers called and duration of calls and files downloaded from the internet) generated on its networks, including business and personal content and communications
- S70. Activity conducted by the company that monitors the use of information systems will comply with the legislative requirements governing the subject
- S71. Serco may use any information it receives via monitoring processes to investigate any claims of breach of this standard or any law, and to instigate appropriate disciplinary or legal proceedings
- S72. Information obtained through monitoring will only be disclosed to a relevant external agency if required by law or those directing the investigation i.e. Serco management, Legal or Human Resources (HR). The information obtained will be held for as long as necessary to complete enquiries, or if part of disciplinary proceedings, in accordance with the relevant retention period
- S73. Wherever reasonable, managers or HR will consult with employees about any suspected breach of this standard before any action is taken. However, this may not always be practical where illegal behaviour or gross misconduct is suspected

3 Responsibilities & Accountabilities

- S74. The following responsibilities will apply to the delivery of the defined standards. If these are not completed effectively, the person responsible will be accountable for any consequences⁶.

Group

- S75. The Group CEO will appoint a Group Information Technology (IT) Lead responsible for:
- developing and maintaining Group Acceptable Use policy
 - ensuring standards and associated procedures and key controls remain fit for purpose, reflect legislative and regulatory requirements and effectively manage acceptable use risks
 - providing oversight and reporting acceptable use performance

Division

- S76. The Divisional CEO will appoint a Divisional IT Lead responsible for:
- implementing acceptable use policy, standards, procedures and key controls across the Division; which may include the development of country/region/Divisional procedures and management systems
 - ensuring procedures and key controls, remain fit for purpose, reflect legislative and regulatory requirements and effectively manage Acceptable Use risks
 - providing oversight of the application of this Group Standard

Contract/Function

- S77. The Contract Manager (or Corporate Function Head) is responsible for:
- Communicating the requirements of the Acceptable Use policy, standards, procedures and key controls
 - Implementing local controls for providing assurance that Acceptable Use risks are being effectively managed

⁶ See Consequence Management Group Standard Ref: SMS-GS-G1

All employees

- S78. All employees are responsible for:
- a. following defined Acceptable Use policy, standards, procedures and work instructions
 - b. telling a line manager of any Acceptable Use concerns

4 Processes and Controls

4.1 Governance processes and controls

Process

A set of related activities that must be carried out to achieve policy outcomes

Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
P1	Acceptable Use responsibilities are defined and understood	⇒ C1	<p>A Group Information Technology (IT) Lead is appointed by the Group CEO with responsibility for:</p> <ul style="list-style-type: none"> Developing and maintaining Group Acceptable Use policy Ensuring standards and associated procedures and key controls remain fit for purpose, reflect legislative and regulatory requirements and effectively manage acceptable use risks Providing oversight and reporting acceptable use performance 	●	○	○	○	○

Process

A set of related activities that must be carried out to achieve policy outcomes

Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
➔ C2	<p>A Divisional IT Lead is appointed by the Divisional CEO with responsibility for:</p> <ul style="list-style-type: none"> Implementing acceptable use policy, standards, procedures and key controls across the Division; which may include the development of country/region/divisional procedures and management systems Ensuring procedures and key controls remain fit for purpose, reflect legislative and regulatory requirements and effectively manage acceptable use risks Providing oversight of the application of this Group Standard 			<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
➔ C3	<p>Contract Managers and Corporate Function Heads are responsible for:</p> <ul style="list-style-type: none"> Communicating the requirements of the Acceptable Use policy, standards, procedures and key controls Implementing local controls for providing assurance that Acceptable Use risks are being effectively managed 			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Process

A set of related activities that must be carried out to achieve policy outcomes

Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
		⇒ C4	All employees are responsible for: <ul style="list-style-type: none"> Following defined Acceptable Use policy, standards, procedures and work instructions Telling a line manager of any Acceptable Use concerns 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
P2	Establish policy	⇒ C5	Policy, standards and Group procedures are defined and published	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		⇒ C6	Policy requirements for acceptable use of information systems are communicated and implemented	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
P3	Establish systems and process	⇒ C7	Appropriate systems and procedures are in place to meet the requirements for acceptable use of information systems and related legal requirements	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		⇒ C8	Systems and procedures are periodically reviewed and updated	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		⇒ C9	Legal and regulatory requirements are monitored with changes reflected in systems and procedures	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Process

A set of related activities that must be carried out to achieve policy outcomes

Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
P4	Compliance assessment and audit	➔ C10	A compliance plan is in place which includes assessment of acceptable use of information systems	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		➔ C11	Compliance and audit reports have action plans to address non-conformities	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		➔ C12	Agreed actions are closed out	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

4.2 Key processes and controls

Process

A set of related activities that must be carried out to achieve policy outcomes

Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Responsibility				
				Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
P5	Raise awareness of policy requirements	↔ C13	All employees have been made aware of Serco's policy and requirements around the acceptable use of information systems	●	●	●	●	○
P6	Monitor use of internet, email, messaging and other information systems	↔ C14	A procedure is in place for appropriate monitoring of the use of internet, email, messaging and other information systems	○	●	○	○	○
P7	Removal of information	↔ C15	A procedure is in place to request the removal of published information	○	●	○	○	○
P8	Manage third parties access to systems	↔ C16	Non-Disclosure/Confidentiality agreements are in place for third parties accessing Serco systems and intranet	●	●	●	●	○
P9	Manage email disclaimer	↔ C17	The standard Serco email disclaimer is attached to the end of emails	●	●	○	○	○
P10	Manage passwords	↔ C18	Passwords comply with password guidelines	●	●	○	○	○
		↔ C19	Passwords are kept safe and not written down, displayed or disclosed to others	●	●	●	●	○

Process

A set of related activities that must be carried out to achieve policy outcomes

Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility

for ensuring controls are in place and operating effectively

Ref	Description		Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
P11	Manage virus protection	➔	C20	All devices which connect to Serco, customer or third party networks or information systems have approved anti-virus software, including a subscription to an update service	●	●	○	○	○
P12	Encryption of PCs/devices and removable media	➔	C21	All PCs/devices and removal media have an approved and appropriate method of encryption, unless permanently located wholly within Serco secure premises, or if the site has been approved by the Divisional Security Lead as secure	●	●	○	○	○

5 Supporting documentation and guidance

The following should be read in conjunction with this standard:

Ref	Document
SMS-GS-G1	Consequence Management Group Standard
SMS-GS-S1	Security Group Standard
SMS-GS-II1	Information and Date Management Group Standard
SMS-GSPOP-II1-2	Document Retention GSOP Code of Conduct

6 Definitions

Term	Definition
Accountability	Being accountable means being not only responsible for something but also answerable for your actions.
Responsibility	<p>A responsible person is the individual who completes the task required. Responsibility can be shared and delegated.</p> <p>All responsible persons will also be accountable for completing tasks effectively. Non-compliance will have consequences which may include disciplinary action as defined within the Consequence Management Group Standard.</p>

Term	Definition
Group	Serco Group plc is the administrative centre of the organisation, responsible for setting corporate strategy, defining governance requirements and supporting the business in its day to day operations
Division	The Group will define a set of business divisions which will be responsible for business delivery within a defined set of markets or geographies.
Business Unit	<p>A Business Unit is a cluster of contracts which provide a similar service e.g. Health, Defence, Transport etc.</p> <p>Where appropriate, a separate legal entity wholly owned or where Serco has a controlling share may also be referred to as a Business Unit, where appropriate.</p> <p>This may also refer to Counties/Territories</p>
Contract	<p>A Contract provides specified requirements to a customer (either directly with Serco or to a consortium/Joint Venture in which Serco is a party)</p> <p>A Contract will also refer to a corporate/functional area.</p> <p>Corporate/functional areas are functions which support the business and they include finance, HR, procurement etc.</p>
Contract Manager	This refers to a manager with responsibility for managing the performance of a contract and can include a Contract Manager on a day-to-day basis (or Operational Manager with devolved responsibility), a Contract Director, Partnership Director and/or Business Unit Managing Director

Term	Definition
BYOD	Bring Your Own Device - the policy of permitting employees to bring personally owned devices (e.g. laptops, tablets, etc.) to their workplace, and use those devices to access and store privileged company or customer information and applications.
Employee	Includes all full-time and part-time employees remunerated by Serco and its subsidiaries, contractors, and consultants.
Information Systems (IS)	All IT and communication systems, equipment and media used by Serco employees (as defined above) to perform their duties and/or publish any information relating to Serco, including, but not limited to the Internet, intranet, social media, email, messaging and telephones.
Protective Marking	Any information marked under a mandated protective marking scheme of the government of the country or territory of operation, customer, partner or vendor.
Removable Media	Refers to storage media which can be removed from its reader device, conferring portability on the data it carries, and includes Memory cards (Compact Flash card, Secure Digital card, Memory Stick), Floppy disks/Zip disks, Magnetic tapes, USB flash drives and external hard drives.
'Serco Restricted and Sensitive'	<p>SRS information is our most valuable information, which, in the wrong hands could cause serious damage to us, our customers, shareholders, partners or suppliers through serious loss of reputation; significant financial loss; loss of opportunity; or legal action.</p> <p>This information may belong to the Company, customers, or third parties. Access to SRS information must be restricted on a need to know basis with only authorised Serco employees, or specified authorised external persons or entities being granted access. Encryption and controls</p>

Term	Definition
	over the distribution outside of Serco must be in place for all SRS information.
'Serco Business'	<p>SB information is information which if disclosed without authorisation, may cause unwanted exposure of the inner-workings of the company, but would not result in significant financial loss or serious harm to the company or its business interests. In essence, it is any information that is not generally made available to the public unless approved for release.</p> <p>This information is generally available within our offices, systems or intranet and all company employees and affiliate employees are permitted to have general access to this kind of information.</p> <p>This information must not be shared beyond the company premises unless with approval for formal business engagement.</p>
Social Media	On-line technologies and practices that people use to share with each other information, opinions and experiences. Social media forms include social networking, Internet forums, message boards, web logs (blogs), wikis, podcasts, pictures and video.
Third Party	An individual who is not an employee of Serco or an organisation that provides labour or services to Serco.

7 Further information and support

If you require any further information or support regarding this Group Standard, or if you have any suggestions for improvement, please contact the Accountable Policy Owner (Group) or email sms@serco.com