Security Standard - Access and Authentication Controls SS-001 (part 1)

Chief Security Office

Department for Work & Pensions

Date: March 2020

1. Revision History

Issue Status	Author	Description	Date
0.1		First Draft	24/01/2017
0.2		Updated with comments and new template	05/05/2017
0.3		Further updates following review comments	22/06/2017
0.4		Amalgamation of several separate standards following review comments.	03/07/2017
1.0		First published version	18/09/2017
1.1		Version for external publication	30/03/2020

2. Distribution

Version	Role/Area	Role	Date

3. Approval History

Issue Status	Approver	Role	Date
1.1		Chief Security Officer	30/03/2020

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted "final" status, and at yearly intervals thereafter.

Contents

4. Introduction

4.1. This Access and Authentication Control Standards document provides the list of controls that are required for business applications, information systems, networks and computing devices.

This list of requirements ensures a baseline level of security that is approved and accepted by the Authority to afford the necessary level of protection to its systems and data.

Furthermore, the security controls presented in this standard are taken from examples of international best practice for information security and have been tailored for the Authority's suitability. This document should be read in conjunction with the Authority's **User Access Control Policy**.

5. Purpose

5.1. The purpose of this document is to enable Suppliers to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to the Authority's security standards, which are based upon international best practice for information security.

5.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

6. Exceptions

In this document the term **MUST** in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption.

6.1. Any exceptions to the application of this standard or where controls cannot be adhered to **MUST** be presented to the Authority where appropriate. This **MUST** be carried out prior to deployment and managed through the design caveats or exception process.

6.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

6.3. Exceptions to this standard **MUST** be maintained on a risk register for accountability, traceability and security governance reporting to the Authority.

7. Audience

7.1. This standard is intended for (but not limited to) Suppliers, security controls testing consultants, solution, domain and security architects and system designers as well as engineers and/or system administrators who are provisioning servers for departmental use.

8. Scope

8.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All of the Supplier's ICT systems, applications, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

8.2. The security control requirements laid out in this standard are product agnostic and applicable for all ICT systems, applications, or service implementations that are provisioned for Authority use.

8.3. Additional controls may be applicable based upon the Security Classification of the information being processed by the Supplier's ICT systems, applications, or service implementations.

8.4. In the event of uncertainty on the controls laid out in this standard please contact the Authority for guidance and support on items which require clarification.

9. Security Controls Assurance

9.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

10. Technical Security Control Requirements

10.1. General Security Control Requirements

Reference	General Security Control Requirement
10.1.1	Controls **MUST** be implemented to restrict access to business applications, information systems, network services, and computing devices, and the information stored on and processed by them.
10.1.2	The Authority and its Suppliers **MUST** implement appropriate identification and authentication controls to manage the risk of unauthorised access, and to ensure the correct management of user accounts and enable auditing.
10.1.3	All individual Supplier information systems, applications, services and networks **MUST** be equipped with and maintain a System Access

Reference	General Security Control Requirement
	Control Policy which **MUST** be approved by the appropriate Information Asset Owners.
10.1.4	The System Access Control Policy **MUST** provide the information that those involved in designing, developing, operating and using the system, application or service will need, in order to ensure that: a) the system, application or service is developed with the appropriate security mechanisms in place; b) That procedures can be developed to support the operation of the system, application or service in accordance with the appropriate security policies and standards.
10.1.5	System Access Control Policies **MUST** be supported by documented procedures, which take account of: a) The Authority's Security Standards, information security classifications, agreements with application owners, requirements set by the owner of systems and legal, regulatory and contractual obligations; b) The need to enforce individual accountability, apply additional control for users with special access privileges, (See also SS-001 pt2 Privileged User Access Control Security Standard), and provide segregation of duties.

10.2. Identity and Access Management Control Requirements

Reference	Identity and Access Management Control Requirements
10.2.1	Identity and access management arrangements **MUST**: a) include a method for validating user identities prior to enabling user accounts b) keep the number of sign-ons required by users to a minimum.
10.2.2	Identity and access management arrangements **MUST** provide a consistent set of methods for: a) identifying users using unique User IDs b) authenticating users using passwords, tokens (smartcards) etc. or biometrics) c) identifying equipment (e.g., by using MAC-based authentication) d) the user sign-on process e) authorising user access privileges f) administering user access privileges.
10.2.3	If possible, identity and access management arrangements **MUST** be developed to improve the integrity of user information by: a) making this information readily available for users to validate b) allowing users to correct their own user information (e.g., by providing users with a self-service application) c) maintaining a limited number of identity stores (i.e., the location where User ID and authentication information is stored, such as a

Reference	Identity and Access Management Control Requirements
	Lightweight Directory Access Protocol (LDAP) directory service, Microsoft Active Directory, or another commercial IAM product) d) using an automated provisioning system (whereby user accounts are created for all target systems, following the creation of an initial entry for a user in a central IAM application) using a centralised change management system.

10.3. Registration Control Requirements

Reference	Registration Control Requirements
10.3.1	Procedures to register and authorise access to an Authority information system, application or service **MUST** be defined and documented in the System Access Control Policy.
10.3.2	The access management functionality **MUST** provide authorised administrators with the ability to create, amend, delete and suspend User accounts.
10.3.3	Access management functionality **MUST** also provide the ability to define the access privileges for the User. See also SS-001 pt2 Privileged User Access Control Security Standard.
10.3.4	Access to an Authority information system, application or service **MUST** not be granted until the authorisation procedures have been completed.
10.3.5	Administrators will, under management direction, set up and maintain control of authorised User accounts and be able to view User account privileges and identifiers on request. Documented instructions **MUST** be provided for Administrators, which detail the procedures that they **MUST** follow.
10.3.6	Administrators **MUST** risk assess whether a two-man rule should be applied for initial enrolment to an authentication system and other precautions applied in accordance with local procedures.
10.3.7	A formal record **MUST** be created, maintained, and be available for examination, of all Users registered to use an Authority information system, application or service.
10.3.8	Where the records are maintained within an Information system, application or service, facilities **MUST** be available to provide reports to management giving details of registered Users and their Access Rights.
10.3.9	A formal record **MUST** be maintained and be available for examination, of all User access privileges awarded, changed or revoked on an Authority information system, application or service. See also SS-001 pt2 Privileged User Access Control Security Standard.
10.3.10	Records **MUST** be maintained of the service accounts and their privileges where: a) special accounts have to be created to allow applications to run; b) access to one system, application or service through the use of service accounts entitles access to additional system, application or service. See also SS-001 pt2 Privileged User Access Control Security Standard.
10.3.11	The records of these service accounts may be maintained automatically by the administration functions of the system, application or service or

Reference	Registration Control Requirements
	manually. Where the records are maintained within an Information system, application or service, facilities **MUST** be available to provide reports to management giving details of Users, including service Users, registered, their access privileges, (See also SS-001 pt2 Privileged User Access Control Security Standard) and changes made.
10.3.12	All access requests **MUST** be retained by the service, for a period 18 months after access is withdrawn.
10.3.13	All user access to Systems of Application **MUST** be recorded and records retained for 6 months.

10.4. Authorisation Control Requirements

Reference	Authorisation Control Requirements
10.4.1	Access to the Authority's information systems, applications or services **MUST** not be authorised until all employment and Basic Personal Security Standard checks have been completed.
10.4.2	The Authority **MUST** approve requests for access to the Authority's network, information systems, applications or services, before access is granted.
10.4.3	The Supplier **MUST** ensure that the user is suitably trained to perform the duties associated with the access being requested.
10.4.4	Supplier information systems, applications or services **MUST** provide facilities to manage Users 'profiles and access privileges based on their role. See also SS-001 pt2 Privileged User Access Control Security Standard.
10.4.5	The User Profiles **MUST** provide the level and detail of information necessary to implement the System Access Control Policy for the system, application or service to ensure that the User will only be granted access to those functions for which approval has been authorised.
10.4.6	The following details **MUST** to be recorded within User Profiles: a) primary/unique USER-ID; b) full name; c) other USER-ID(s) if needed to access local and/or remote resources; d) address(es); e) User status (new, suspended, terminated, re-certification required, on-leave, etc.); f) key dates (e.g. User account start, termination, last-changed, re-activation); g) group, job or other role/responsibility codes that grant indirect resource access authorisations; h) all authorised Access Rights; i) any encryption key data, protected encryption servers, credential holders, etc. (if used); j) method(s) of authentication (password, biometric or other credential types and authentication details).

Reference	Authorisation Control Requirements
10.4.7	Supplier information systems, applications or services **MUST** provide facilities to control access to the system, application or service based on a User's privileges, as defined by their profile.
10.4.8	The system, application or service **MUST** not perform any actions on behalf of a User unless the User has been positively authenticated.
10.4.9	The system, application or service **MUST** provide the User with a password as one factor of authentication.
10.4.10	The User access **MUST** be restricted to the minimum necessary to satisfy business needs according to their defined profile / role.

10.5. Sign-on Process Control Requirements

Reference	Sign-on Process Control Requirements
10.5.1	There **MUST** be a sign-on process that users need to follow before they are provided with access to information systems, which **MUST** enable individual users to be identified (e.g., using unique user IDs).
10.5.2	Sign-on mechanisms **MUST** be configured so that they: a) validate sign-on information only when it has all been entered; b) limit the duration of any one sign-on session; c) are re-enabled automatically after interruption (i.e., the sign-on process is required again following a disconnection from the application).
10.5.3	Sign-on mechanisms **MUST** be configured to provide information so that they: a) display no identifying details until after sign-on is completed successfully; b) warn that only authorised users are permitted access; c) record all successful and unsuccessful sign-on attempts; d) advise users (on successful sign-on) of the date/time of their last successful sign-on and all unsuccessful sign-on attempts since their most recent successful sign-on.
10.5.4	Sign-on mechanisms **MUST** be configured to protect authentication details against unauthorised disclosure by using: a) cryptographic hashing algorithms to conceal clear text passwords and resist brute force attacks b) salting methods to ensure each password hash is unique to resist attacks using rainbow tables.
10.5.5	Sign-on mechanisms **MUST** be configured to delete authentication details when they are no longer required by the authenticating system, such as immediately following successful authentication.
10.5.6	The approval of the Authority **MUST** be obtained before any important features of the sign-on process are bypassed, disabled or changed.

10.6. Access Review Control Requirements

Reference	Access Review Control Requirements
10.6.1	Where an individual is leaving, their account **MUST** be deactivated on the day after their employment or contract ends.
10.6.2	All deactivated accounts **MUST** be deleted within 12 months of the account being deactivated.
10.6.3	Quarterly reviews **MUST** be carried out of all leavers, both permanent and contractors, to confirm accounts have been deactivated.
10.6.4	Quarterly reviews **MUST** be carried out of all User accounts, looking for accounts that have been deactivated for more than 12 months. Any such accounts found **MUST** be deleted**.**
10.6.5	Where a user is absent from work for a period greater than six months (due to secondment, courses, maternity leave, long term sickness absence etc.) the account **MUST** be deactivated.
10.6.6	Quarterly reviews **MUST** be carried out of all User accounts looking for accounts that have been dormant for more than 100 days. Where such accounts are detected the relevant line manager **MUST** be contacted to confirm whether the account is still required, and action **MUST** be taken to either deactivate or delete the accounts.

10.7. Authentication Control Requirements

Reference	Authentication Control Requirements
10.7.1	Access to the Authority's applications, systems, networks, services and computing devices **MUST** be restricted to authorised individuals by the use of access control mechanisms. Access control mechanisms typically involve the submission of two pieces of information to prove an identity: a unique identifier (e.g., user ID or a user's email address) and a corresponding authenticator (e.g., a password, digital certificate or fingerprint scan). Access control mechanisms are often classified in terms of the factors that are used to authenticate users, and are based upon something the user: – knows (e.g., a password) – has (e.g., physical token, smartcard or digital certificate) – is or does (e.g., biometrics such as fingerprint, iris pattern, hand geometry, voice characteristic or writing style). As industry best practice, two factor authentication, (2FA), **MUST** be considered and, where it is a proportionate counter measure to risk, preferred when determining authentication control requirements for internal user access to the Authority's applications, systems, network services, or computing devices.
10.7.2	All individual Supplier information systems, applications, services and networks **MUST** be equipped with and maintain a System Access Control Policy which **MUST** include a Password Management Section, which defines the parameters for the selection and use of passwords or

Reference	Authentication Control Requirements
	PINs, developed in accordance with NCSC Password Guidance: Simplifying Your Approach August 2016.
10.7.3	If possible machine-generated passwords **MUST** be the preferred option because they eliminate those passwords that would be simple for an attacker to guess, they require little effort from the user to create, and, depending on the generation scheme, can produce passwords that are fairly easy to remember.
10.7.4	If user-generated passwords are used, the Password Management section of the System Access Control Policy must consider proportionate and appropriate values for password construction ensuring: i. structure and format – enforcing the requirement for complex character sets in passwords is NOT recommended. Instead, technical controls **MUST** be implemented defending against automated guessing attacks by either using account lockout, throttling, or protective monitoring - blacklisting the most common password choices; ii. frequency of change - regular password changing harms rather than improves security, so placing this burden on users **MUST** be avoided. However, users **MUST** change their passwords on indication or suspicion of compromise; iii. passwords **MUST** not be dictionary words or the same as the User ID. iv. Users **MUST** be able to change their own password after re-entering their current password; v. authorised roles / functions **MUST** be able to initialise or change passwords for Users; vi. New passwords **MUST** be entered twice to avoid keying errors;
10.7.5	New User accounts **MUST** have passwords set before the account is enabled.
10.7.6	Default or temporary passwords **MUST** expire at first logon before access to system, application or service resources by a new User is allowed.
10.7.7	Passwords **MUST** not be stored, transmitted or otherwise expressed in a clear text e.g. human or machine readable format, by any process handling the password.
10.7.8	Passwords **MUST** be stored as a hash of the password value using an approved hashing algorithm with a salt added to the password before hashing.
10.7.9	Files containing hashed passwords **MUST** be hidden by the system, application or service.
10.7.10	Users **MUST** be notified in advance to change their password prior to its expiry date.
10.7.11	Systems and applications **MUST** enforce all password parameters.
10.7.12	The allocation of passwords **MUST** be controlled and the process documented in the system Access Control Document.
10.7.13	Passwords **MUST** only be issued to users when their identity has been confirmed.

Reference	Authentication Control Requirements
10.7.14	The confidentiality of passwords **MUST** be maintained when the passwords are being distributed.
10.7.15	The protection afforded to passwords during distribution **MUST** be at least appropriate to the classification of the information protected by the passwords.
10.7.16	If a password is being distributed electronically, it **MUST** be sent via a route accepted as 'trusted' or secure or in an approved encrypted format.
10.7.17	If a password is being distributed by post, it **MUST** be sent to a pre-defined location for the User.
10.7.18	User ID information **MUST NOT** be included in any communication to a User alongside reference to a password.
10.7.19	If a password is being distributed by telephone, it **MUST** be to a known telephone number for the User, and the identity of the User **MUST** be authenticated before the password is divulged.
10.7.20	Where the default configuration of hardware or software includes accounts with default passwords, these passwords **MUST** be changed before the Supplier's information system, application or service is brought in to use.

10.8. Token Management

Reference	Token Management
10.8.1	Token Management Procedures **MUST** ensure that Physical Security Tokens are properly managed at each stage of their lifecycle and **MUST** cover irregularities such as loss, theft or damage.
10.8.2	Token Management Procedures **MUST** cover: a) Ordering; b) Storage; c) Distribution; d) Allocation; e) Recovery; f) Destruction; g) Actions required as a result of loss, theft or damage.
10.8.3	Users **MUST** only be issued with one security token for a specific system, application or service, with the exception where authorised Privileged User access is dependent upon a second token. In this latter case, the second token **MUST** only be released or returned under formal change control. See also SS-001 pt2 Privileged User Access Control Security Standard.
10.8.4	A security token **MUST** only be associated with one User identity. This is necessary to ensure that a User's actions are fully accountable.
10.8.5	Users **MUST** be instructed to immediately report any lost or stolen tokens.
10.8.6	The process for registering new token Users and issuing them with tokens that **MUST**:

Reference	Token Management
	a) ensure that passwords relating to tokens are not sent in the form of clear text (e.g., in email or text messages) and not sent together with the token b) directly involve the person to whom the token uniquely applies (e.g., face-to-face registration in a secure location) c) verify the identity of the User, such as inspecting official identity documentation or through independent confirmation.
10.8.7	Users of token authentication **MUST** be advised to: a) keep passwords for access to tokens confidential (i.e., to avoid making them visible to others by writing them down or disclosing them to others) b) protect tokens against loss, theft and misuse (e.g., avoid sharing with unauthorised individuals) c) report if the tokens have been or are suspected of being compromised (e.g., tampered with).

10.9. Additional Supplier Access Control Requirements

Reference	Additional Supplier Access Control Requirements
10.9.1	Supplier access to the Authority's applications, systems or services **MUST** not be granted until a contract is in place.
10.9.2	Supplier access to the Authority's applications, systems or services **MUST** not be granted until a risk assessment and Supplier assessment has been completed.
10.9.3	All Supplier access requests **MUST** be approved by the Authority
10.9.4	All access requests **MUST** be retained for a minimum period of 12 months.
10.9.5	Supplier access accounts **MUST** not be permanently active and **MUST** be disabled when access is not required. There **MUST** be a documented procedure covering requests to enable the account.
10.9.6	Two factor authentication **MUST** be used for all Supplier Accounts.
10.9.7	All Supplier access **MUST** be monitored real-time.
10.9.8	All Supplier access to applications, systems or services **MUST** be recorded and records retained for 12 months.
10.9.9	All Supplier actions within applications, systems or services **MUST** be recorded and records retained for 12 months.
10.9.10	Application, system or service owners **MUST** review Supplier accounts every 6 months to confirm access is still required.
10.9.11	Supplier access **MUST** be terminated immediately at the end of the contract.
10.9.12	Suppliers with access to the Authority's applications and systems **MUST** be subject to annual Supplier audit.

10.10. Customer Access Security Requirements

Reference	Customer Access Security Requirements
10.10.1	Applications, systems and services owners **MUST** document the evidence required to identify an individual as part of the registration process.
10.10.2	Identification Assurance **MUST** be in accordance with two Government Digital Service (GDS) Good Practice Guides (GPG): GPG 44 – Authentication and Credentials for use with HMG Online services; GPG 45 – Identity Proofing and Verification (IPV) of an Individual. These are publicly available on the GOV.UK website..
10.10.3	Customer accounts **MUST** not be activated until identity is proved.
10.10.4	Customer user IDs **MUST** be easy for the user to remember and unique to the individual
10.10.5	Passwords and password management **MUST** comply with the Password Management Access Control Standard
10.10.6	The Customer **MUST** be forced to change password on first login
10.10.7	Customer **MUST** be forced to change their password at least every 12 months

10.11. Generic Accounts Security Control Requirements

Reference	Generic Accounts Security Control Requirements
10.11.1	Generic or shared accounts **MUST not** be used to carry out any activities which may be achieved using other individually assigned privileged accounts.
10.11.2	Generic or shared accounts **MUST** only be used to carry out activities which cannot be achieved by other means.
10.11.3	Suppliers are responsible for ensuring the appropriate and necessary use of generic or shared accounts by their staff.
10.11.4	All generic or shared account accesses **MUST** be subject to a technical risk assessment and authorised in writing by the Authority or be directly associated with a planned activity e.g. Service Desk Change Request or Incident.
10.11.5	The Supplier **MUST** regularly check to ensure that no unauthorised account access has taken place.
10.11.6	While all account usage is subject to monitoring, the use of generic or shared accounts **MUST** not only be monitored, but **MUST** always be subject to audit.

11. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

12. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However, it is deemed that Suppliers implementing this standard are obliged to incorporate accessibility functions.

13. Reference Documents

SS-001 Security Standard part 2 – Privileged User Access Controls

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

14. Definition of Terms

Privileged User	A Privileged User is a user who has an elevated level of access to a network, computer hardware or system components or functionality and is authorised to perform functions that standard and elevated users are not authorised to perform.
Business Application	Business application is an Authority owned software programme used by Authority staff or Authority customer to perform Authority business functions such as JSA Online. It does not include MS Office applications.
Information System	Information System is an Authority owned software infrastructure used by Authority staff or Authority customer to perform Authority business functions such as Universal Credit
Information Service	Business application owned by a Supplier but used by Authority staff or Authority customer to perform Authority business functions such as a hosted learning management system
Service Account	An account provisioned for use mainly or solely by applications or services rather than a human user.
User Account	An account provisioned for use by human users.

15. Glossary

DA	Design Authority (DA)
Authority	The Authority is the Department for Work and Pensions (DWP)
Supplier	Is inclusive of Contractor, their employees or any sub-contractors used