Taking over a system

A handover checklist

Taking over a system: a handover checklist

A system belongs, in practice, to whoever holds its accounts. This brief sets out what to move, check and write down before the supplier or developer who built it leaves.

Written for an organisation whose supplier or sole developer is leaving, or which wants to own the software it paid for, and for the person inside it who will be accountable afterwards.

Access and ownership

When the person who built a system leaves, the system stays where they put it: the code in their repository, the hosting in their cloud account, the domain in their name. The NCSC asks organisations to maintain a list of suppliers and what assets they hold, and to consider the impact of someone else taking control of the domain name. Each line below needs a named person inside the organisation and a date. Day one is the first day the system runs without the outgoing supplier.

The common assumption is that an organisation owns the software it paid for. Under the Copyright, Designs and Patents Act 1988, a computer program is a literary work and its author is the first owner of the copyright. The exception is work made by an employee in the course of employment, which belongs to the employer unless agreed otherwise. A supplier is not the customer's employee, and an assignment of copyright is not effective unless it is in writing, signed by or on behalf of the assignor. Whether a given contract did that is a question for a lawyer.

Item	What the organisation should hold	Owner, and by when
Code repositories	Every repository with its full history, in an account the organisation controls, not a copy of the latest files.	Accountable person, before the supplier leaves
Hosting and cloud accounts	The owner login and the billing, in the organisation's name.	Accountable person, before the supplier leaves
Domains and DNS	The organisation as registrant, with the registrar and DNS logins held inside it.	Accountable person, before the supplier leaves
Admin credentials	Every admin, deployment and service credential, who holds each, and when it will be changed.	Accountable person, day one
Third-party licences	Each paid component and service, whose name it is in, and its renewal date.	Finance, before the first renewal

Item	What the organisation should hold	Owner, and by when
Intellectual property	A written, signed assignment of copyright in the code, or the licence under which the organisation uses it.	Contract owner, before the final payment
Data export	A full export in a documented format. A supplier processing personal data must be bound by contract to delete or return it at the end, at the organisation's choice (UK GDPR Article 28(3)(g)).	Data protection lead, before notice ends

Technical state

The NCSC attributes the majority of cyber security incidents to attackers exploiting publicly disclosed vulnerabilities. The common assumption is that a system reporting no pending updates is up to date. The NCSC notes that software asset management suites might not check software libraries and dependencies. A handover is the point at which to find out what the system is made of.

- [ ] Every runtime, framework and database listed with its end-of-support date. After those dates no security updates are published; the NCSC advises planning migration as the date approaches, and segregating unsupported high-risk systems that cannot be upgraded.
  NCSC, 10 Steps to Cyber Security: vulnerability management
- [ ] A dependency scan of every repository.
  NCSC, 10 Steps to Cyber Security: vulnerability management
- [ ] A named person applying, within 14 days of release, each update that fixes a critical, high-risk or unrated vulnerability, with a rollback route for an update that fails. The 14 days is a Cyber Essentials requirement; the scheme asks for updates as soon as possible, and puts bespoke and custom components of web applications out of scope.
  NCSC, Cyber Essentials requirements v3.3, section 3 and scope (vii); NCSC, 10 Steps: vulnerability management
- [ ] One backup restored before sign-off. The NCSC's advice is to know how to restore a backup and to check that it contains all the important data.
  NCSC, Small organisations guide: backing up your data
- [ ] Alerts and logs reaching someone inside the organisation, who can search them.
  NCSC, 10 Steps to Cyber Security: logging and monitoring

Where the system holds personal data, the restore is also a legal question. The ICO's guidance says UK GDPR requires the ability to restore availability and access to personal data in a timely manner after a physical or technical incident, and a process for regularly testing the effectiveness of security measures. The guidance is under review after the Data (Use and Access) Act.

> The test of documentation is whether someone other than its author can deploy the system from it. None of the sources cited here sets that test. It shows whether the system still depends on a single person.

People and process

Much of what keeps a system running is held in one person's head. Before the last day, write down how a release is made, how a backup is restored, what has broken before and which third parties are called. The NCSC asks for suppliers' contact details to be held and accessible during an incident, and tells small organisations not to leave responsibility for cyber security with a single person.

The common assumption is that passwords should be changed on a schedule. The NCSC advises against regular expiry, and asks instead for an effective leavers process, and for a shared password to be changed when someone is no longer allowed access. A departing supplier is that case: every password and key they held is changed on day one, and accounts no longer needed are removed or disabled, which is a Cyber Essentials requirement.

The first thirty days are for proving the lists, not extending the system: one release and one restore, each made by someone other than the person who left, and a check that none of that person's credentials still works. Thirty days is a planning horizon, not a standard.

Sources

Copyright, Designs and Patents Act 1988, c. 48, section 3(1), definition of literary work. legislation.gov.uk, revised text, no known outstanding effects, retrieved 19 September 2026.

Copyright, Designs and Patents Act 1988, c. 48, section 11(1) and (2), first ownership of copyright. legislation.gov.uk, revised text, no known outstanding effects, retrieved 19 September 2026.

Copyright, Designs and Patents Act 1988, c. 48, section 90(3), assignment. legislation.gov.uk, revised text, no known outstanding effects, retrieved 19 September 2026.

NCSC, 10 Steps to Cyber Security: Asset management, published 11 May 2021, version 1.0. Domain names, the supplier list and contact details.

NCSC, 10 Steps to Cyber Security: Vulnerability management, published 11 May 2021, version 1.0. Exploited vulnerabilities, rollback, end of support, libraries and dependencies, and segregation.

NCSC, 10 Steps to Cyber Security: Logging and monitoring, published 11 May 2021, version 1.0. Log access.

NCSC, Small organisations guide to cyber security: Backing up your data, published 9 April 2026, reviewed 21 July 2026. Restoring backups.

NCSC, Small organisations guide to cyber security, introduction, published 9 April 2026, reviewed 21 July 2026.

NCSC, Password administration for system owners: Password policy, updating your approach, reviewed 19 November 2018. Password expiry, leavers and shared passwords.

NCSC, Cyber Essentials: Requirements for IT Infrastructure v3.3, April 2026, effective from 27 April 2026. Section D scope (vii); section 3, Security Update Management; section 4, User Access Control.

Information Commissioner's Office, A guide to data security (UK GDPR Article 32), latest update 19 May 2023, marked as under review. Restoring availability and testing measures.

Information Commissioner's Office, Contracts and liabilities between controllers and processors: What needs to be included in the contract?, End-of-contract provisions, marked as under review after the Data (Use and Access) Act.

What this brief is not

This brief is not legal advice, and completing it certifies nothing: it does not make a system compliant with Cyber Essentials or UK GDPR. It reports what those sources say, with references, so that a reader can check them and take advice on their own contracts. It is not a case study and describes no organisation. We build and maintain software, and the checklist should be used as readily against us as against any other supplier.

Theo Coleman
Chief Technology Officer, BespokeWorks. August 2026