Nextcloud 11

Assurance Statement

Background

One of Nextcloud's key objectives is to maintain a high level of customer confidence by continually assessing the security controls in place that would be expected of any organisation providing this type of service. Nextcloud has dedicated security experts continuously working with the Nextcloud solution and supporting service to ensure that the security features designed and deployed provide the appropriate security layers to mitigate risk from the most common security problems.

The Nextcloud edition 11 provides many new security related features (Full list below), such as enhancement of Access Controls, data in transit protection, strengthening of password logic. All of which enrich the Nextcloud servers security layers with minimum impact on the user.

These Security layers are designed, built and deployed on industry standards using Secure-Software Development Lifecycle processes and best practice ideology.

Security features for the new Nextcloud 11 release are;

- Two Factor Authentication using U2F / TOTP ✓
- Bruteforce protection ✓
- Content Security Policy v3.0 Support (with nonce instead of "self" for script-src) ✓
- Same-Site cookies support ✓
- Password confirmation for sensitive actions (e.g. when changing email or passwords) ✓
- Same-Site cookies are prefixed with __Host ✓
- Improved password reset logic ✓
- Use HTTPS by default if no protocol is given ✓
- Application specific tokens can be forbidden file system access ✓

Table 1: Nextcloud 11 Security Features

Assurance

Many consumers when considering new web-services, premise or Cloud hosted applications, IaaS (infrastructure), SaaS (Software), private or public Cloud services etc. will decide which key principles of assurance are important, and how much (if any) assurance they require in the implementation and consumption of these services. Nextcloud understands the necessity to provide core principle baseline security requirements, as such Nextcloud 11 is built on these security principles to ultimately deliver a secure solution to their customers.

Risk Management

Risk is assessed by Nextcloud based on current industry standards such as Clause 14 of ISO/IEC27001-2013 and key security principles that are common to many services such key Cloud Security principles. From a technical perspective Nextcloud 11 is subject to in-house Vulnerability Management and routine independent penetration testing using industry certified suppliers. There are also independent reviews of Operational Security and Governance related to Nextcloud's design and includes reviewing policy, process and related procedures.

Nextcloud has assessed the threat against three core areas, as highlighted below; the principle control areas are presented in Table 2 below;
1 - People - i.e. Customers / consumers, Nextcloud internal users and external users, hackers; developers;
2 - Technology - attacks designed to exploit vulnerabilities in software; the design;
3 - Environment - take advantage of weaknesses in poor management, and weak governance in order to compromise the service.

Principle;	**Control area;**
ISO/IEC27001:2013;	- Secure Development Policy.
	- System Change Control procedures.
	- Technical review of applications after operating platform changes.
	- Restrictions on changes to software packages.
	- Secure system engineering principles.
	- Secure development environment.
	- Outsourced development.
	- System security testing.
	- System acceptance testing.
Cloud Security Principles	- Data in Transit.
	- Protection and resilience in the design.
	- Governance framework.
	- Operational Security.
	- Secure development.
	- Personal security.
	- Identity and Authentication.
	- Secure service administration.
Independent testing	- Validation of application and services.

Table 2: Baseline industry standards and Security Principles

Nextcloud Assertions

Nextcloud makes the following services assertions based on ensuring the Confidentiality, Integrity and Availability of the Nextcloud solution and service. Whilst Nextcloud does not process or host any customer data Nextcloud is aligned to the Legal and compliance requirements of the EU GDPR Data Protection legislation.

Common approaches to assurance provide a number of means by which the "level" or "strength" of assurance can be assessed. These approaches are described in the following areas.

Nextcloud Service Provider Assertion

Nextcloud understands that consumers are reliant on the honesty, accuracy and completeness of the service provider's assertions. Nextcloud assurance is based on:

- *A good level of maturity around security;*
- *The existence of in-house security team members and stakeholders;*
- *Proactive testing and historical evidence of responding to and managing security issues.*

Independent Validation of Nextcloud Assertions

An independent third party reviews and confirms the Nextcloud assertions.

- *NCC Group have conducted a review of Nextcloud alignment to core principles of security based on the Security Principles (detailed in Table 2).*
- *Independent 'Penetration tests' by Veracode have been conducted and all risks mitigated and managed in accordance with Nextcloud policy.*
- *Internal Vulnerability scanning and risk management*

Certification and implementation of controls reviewed by a qualified individual(s).

Suitably qualified individuals will review the scope of the applied security controls. This approach provides a higher degree of confidence that the service meets the stated objectives through alignment against an appropriate standard.

Independent Testing of Implementation

Testing supply chain used has appropriate industry recognised certification and qualifications for the testing they are carrying out. Nextcloud understands that Independent testing provides confidence that the design, service implementation achieves the objectives and reduces the reliance on supplier assertions. The results of testing reflect the design, service at a particular moment in time; routine testing is undertaken including testing as the service evolves.

Assurance in the service design

Nextcloud employing certified Architects to provide confidence in the design (and implementation of its recommendations) will give confidence that:

- *the design and security features defends against common attacks;*
- *the proposed security controls are appropriate;*
- *The proposed architecture would allow effective secure operation of the service.*
- *The solutions design will be subject to on-going independent penetration tests by an approved accredited company.*

End of Statement