

SECURITY STANDARD

Table Of Contents

1	Overview and Definitions	1
2	Security Implementation Plans	1
3	Minimum Requirements	2
3.1	Security Management	2
3.1.1	Information Security Policy	2
3.1.2	Security Representative	2
3.1.3	Security Awareness	2
3.1.4	Incident Response	3
3.2	Identification and Authentication	3
3.2.1	User Identification and Authentication	3
3.2.2	Authentication and Password Management	3
3.3	Access Controls	5
3.3.1	Account Management	5
3.3.2	Access Approval Process (System-Level Access)	5
3.3.3	Supervision and Review – Access Control	6
3.4	Audit and Accountability	6
3.4.1	Logging and Audit Requirements for Fully Participating Libraries and Host Sites	7
3.4.1.1	Auditable Events	7
3.4.1.2	Content of Audit Records	7
3.4.1.3	Protection of Audit Information	8
3.4.1.4	Audit Record Retention	8
3.4.2	Marking of Image Files	8
3.4.3	Forensic Analysis	9
3.5	Network Security	9
3.5.1	Electronic Perimeter	9
3.5.2	Network Firewall	10
3.5.3	Device Hardening	10
3.5.4	Network Security Testing	10
3.5.5	Remote Network Access	11
3.5.6	Encryption of Digitized Files	11
3.6	Media Protection	12
3.6.1	Media Access	12
3.6.2	Media Inventory	12
3.6.3	Media Storage	12
3.6.4	Media Sanitization and Disposal	13
3.7	Physical and Environmental Protection	13
3.7.1	Physical Access Authorizations	13

**Attachment D
to Amended Settlement Agreement**

3.7.2	Physical Access Control	14
3.7.3	Visitor Control	14
3.7.4	Access Records	14
3.8	Risk Assessment	14
3.8.1	Risk Assessment	14
3.8.2	Vulnerability Management	15
3.9	Digitized File Content Delivery by Google	15
3.9.1	Preview Uses	15
3.9.2	Consumer Purchase	16
3.9.3	Institutional Subscription	16
3.10	Access to Research Corpus by Host Sites	17
3.11	Use of Library Digital Copy by Fully Participating Libraries	17

AWAITING
COURT
APPROVAL

1 Overview and Definitions

This is the Security Standard required by the Amended Settlement Agreement.

Definitions:

“Authorized Personnel” of a Responsible Party means the employees, vendors, contractors and business partners of the Responsible Party who access (i) unencrypted Digitized Files or systems storing unencrypted Digitized Files, and (ii) encrypted Digitized Files or systems storing encrypted Digitized Files to the extent such persons have access to the applicable encryption keys, in both cases, for the purpose of maintenance, support or development. The term “Authorized Personnel” does not include End Users.

“Digitized Files” refers (i) in the case of Google, to electronic files of Books Digitized by or for Google, or provided to Google and used under the authorizations granted to Google in the Amended Settlement Agreement, (ii) in the case of Fully Participating Libraries, to electronic files that are included in any LDC, or (iii) in the case of Host Sites, to electronic files that are included in the Research Corpus and, for each of the foregoing clauses (i) – (iii), unless otherwise specified, include only the individual image files and the OCR output from such electronic files. This definition of Digitized Files does not include electronic files to the extent Google uses such files pursuant to then-in-effect agreements directly with individual Rightsholders (e.g., through the Partner Program).

“End Users” means Google’s end users and does not include Authorized Personnel.

“Responsible Party” means the Person that is required to comply with this Security Standard in accordance with Article VIII of the Amended Settlement Agreement, the Library-Registry (Fully Participating) Agreement and the Host Site-Registry Agreement and, as the context requires, shall refer to Google, a Fully Participating Library or a Host Site.

All other capitalized terms used, but not defined, in this Security Standard have the same meanings as in the Amended Settlement Agreement.

2 Security Implementation Plans

In accordance with Article VIII of the Amended Settlement Agreement, Google, each Fully Participating Library and each Host Site is required to formulate a Security Implementation Plan that meets the requirements of this Security Standard.

3 Minimum Requirements

This Section includes the minimum requirements that the Responsible Party shall use in protecting unencrypted Digitized Files.

3.1 Security Management

The requirements under this heading pertain to the ability of the Responsible Party to oversee and manage the information security program and associated controls through policies, personnel, training and procedures.

3.1.1 Information Security Policy

Establish (if not already in place), publish, maintain and disseminate information security policies that address all of the requirements contained herein and that are disseminated to all relevant Authorized Personnel. These policies shall be reviewed annually and updated when necessary. Information security policies are approved annually and after each revision by the appropriate management in the Responsible Party's organization. Maintain appropriate records of such approval.

3.1.2 Security Representative

Each Responsible Party that has custody of unencrypted Digitized Files is to have a formally appointed employee ("Information Security Representative" or "ISR") that understands the policies and procedures used to specifically control sensitive areas and information. The ISR will acknowledge his/her responsibilities and the Responsible Party will keep a record of such acknowledgement.

3.1.3 Security Awareness

Implement (if not already in place) a security awareness program for all Authorized Personnel that will include a review upon hire, and retraining at least every three (3) years. The Responsible Party will keep a record of such retraining and acknowledgements by such Authorized Personnel that they have been retrained.

Authorized Personnel shall be informed that systems contain sensitive copyrighted material and that access to such material is restricted and subject to specific access controls.

3.1.4 Incident Response

Maintain security incident response plans that will address the response procedures, roles and responsibilities, and communication with contact details.

In accordance with Section 8.3 of the Amended Settlement Agreement, each Responsible Party is required to promptly report to the Registry all breaches of its Security Implementation Plan other than Inconsequential Breaches. Breaches that pose a reasonable risk of exposing unencrypted Digitized Files, and all other breaches that are not Inconsequential Breaches, shall be tracked. All such breaches, as well as Inconsequential Breaches resulting in either disciplinary action or changes to the Responsible Party's information security policies, shall be disclosed by the Responsible Party during an audit.

3.2 Identification and Authentication

Requirements under this heading pertain to the controls that require the Responsible Party's Authorized Personnel, management and administrators to have an authorized account on the network and/or systems when accessing unencrypted Digitized Files. To use those accounts, each such user must have a unique identifier and a means of authenticating his/her identity.

3.2.1 User Identification and Authentication

Passwords, passphrases, digital keys or other similar methods ("Credentials") are used to authenticate System-level Access to systems storing and processing unencrypted Digitized Files.

3.2.2 Authentication and Password Management

Ensure proper user authentication and password management for access to unencrypted Digitized Files and their associated data stores, applications and tool sets.

Authentication and password management controls in this Section should adhere to FIPS 112, Section 4.2 – Password System for Medium Protection Requirements of the National Institute of Standards Technology ("NIST"), with the exception that passwords shall not be transmitted in cleartext. If, however, a Responsible Party does not adhere to FIPS 112 Section 4.2, then it

**Attachment D
to Amended Settlement Agreement**

shall implement authentication and password management controls that provide protection equivalent to such standard with respect to protecting the security of the unencrypted Digitized Files and that do not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible Party implements authentication and password management controls that provide such equivalent level of protection, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any difference between the requirements of FIPS 112 Section 4.2 and the Responsible Party's actual authentication and password management controls, (ii) provide a business justification for each such difference, and (iii) demonstrate that such implementation provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

- Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- Immediately revoke access for any Authorized Personnel who are terminated.
- Do not permit Authorized Personnel to share their unique accounts.
- Put in password change policies and procedures. Educate Authorized Personnel about these policies and require that they change their passwords when appropriate.
- Require Authorized Personnel to use passwords that cannot be easily guessed or brute-forced.
- Require idle sessions to be logged out or screens to be locked after a reasonable period of time if they are left unattended.
- Require authentication for access to any data storage containing unencrypted Digitized Files. This includes access by applications, administrators, and all other support personnel.

3.3 Access Controls

The requirements under this heading pertain to the ability of the Responsible Party to control access to unencrypted Digitized Files, to limit that access only to Authorized Personnel, and to further limit what actions Authorized Personnel may take with unencrypted Digitized Files. Access controls should adhere to the Moderate Controls for AC-1, AC-2 and AC-3 of Appendix F of NIST 800-53 – The Security Control Catalog. If, however, a Responsible Party does not adhere to such standard, then it shall implement access controls that provide protection equivalent to such standard with respect to protecting the security of the unencrypted Digitized Files and that do not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible Party implements access controls that provide such equivalent level of protection, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any difference between the requirements of the Moderate Controls for AC-1, AC-2 and AC-3 of Appendix F of NIST 800-53 and the Responsible Party’s actual access controls, (ii) provide a business justification for each such difference, and (iii) demonstrate that such implementation provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

3.3.1 Account Management

Access (“System-level Access”) for the set-up and maintenance of hardware and software of systems storing and processing unencrypted Digitized Files requires Authorized Personnel to log in.

3.3.2 Access Approval Process (System-Level Access)

The Responsible Party will implement a process to manage System-level Access to unencrypted Digitized Files. This process will encompass the following:

- The Responsible Party will select persons (“Access Approvers”) who will be responsible for approving System-level Access to systems containing unencrypted Digitized Files.
- No person shall be granted System-level Access to systems where unencrypted Digitized Files are stored unless such access has been approved by an Access Approver.

- Access Approvers may only approve System-level Access for personnel who require it for the purpose of providing system maintenance or to perform appropriate job duties.
- Access is removed for Authorized Personnel no longer requiring System-level Access to the systems where unencrypted Digitized Files are stored or processed.
- Authorized Personnel leaving the employment of the Responsible Party have their System-level Access removed at the time of termination.
- The System-level Access rights of any Authorized Personnel will be suspended if the Responsible Party becomes aware of or has reason to believe that such individual is involved in inappropriate access to unencrypted Digitized Files.
- A list (“Authorization List”) of Authorized Personnel authorized to have System-level Access to systems storing or processing unencrypted Digitized Files is actively maintained, managed, and available to the ISR or his/her delegate.

3.3.3 Supervision and Review – Access Control

The Authorization List is reviewed on a yearly basis, and acknowledged by the ISR or his/her delegate.

3.4 Audit and Accountability

The requirements under this heading pertain to the ability of an applicable Responsible Party to (a) record the actions of Authorized Personnel, if required, (b) identify the source of an Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access, as applicable, and (c) conduct forensic analysis regarding any such breach. If, however, a Responsible Party does not adhere to these requirements, then it shall implement controls that provide protection equivalent to such requirements with respect to protecting the security of the unencrypted Digitized Files and that do not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible Party implements controls that provide such equivalent level of protection, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any

difference between the requirements of this section and the Responsible Party's actual controls, (ii) provide a business justification for each such difference, and (iii) demonstrate that such implementation provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

3.4.1 Logging and Audit Requirements for Fully Participating Libraries and Host Sites

The requirements under this heading pertain to the ability of the Fully Participating Libraries and Host Sites (other than Google) to record the actions of Authorized Personnel described in this Section.

3.4.1.1 Auditable Events

Fully Participating Libraries and Host Sites (other than Google) will record the following events relating to access of unencrypted Digitized Files, and maintain such information in logs:

- Authentication events
- File access events
- Administrative events

3.4.1.2 Content of Audit Records

Audit log records of Fully Participating Libraries and Host Sites (other than Google) relating to access to unencrypted Digitized Files will contain the following:

- Date and time of event
- User responsible for event
- Object of event (file name, database field, etc)
- Type of event

All systems used to support the audit logging function must have the current internal system time accurately reflected and synchronized to a single time source to ensure time is

constant across all delivery systems for event logging. Automated methods should be used to ensure time is synchronized.

3.4.1.3 Protection of Audit Information

Fully Participating Libraries and Host Sites (other than Google) will ensure that audit files and audit evidence relating to the access to unencrypted Digitized Files are protected from inappropriate modifications.

3.4.1.4 Audit Record Retention

Audit logs relating to access to unencrypted Digitized Files are to be maintained and readily available for a period of time reasonably necessary, but, in no event, less than six (6) months, to allow access to be traced in case of an incident. Such logs must also be maintained for at least an additional six (6) months thereafter. Each Security Implementation Plan shall specify the period of time such logs will be maintained.

3.4.2 Marking of Image Files

Google will take the following measures to identify the source of a security breach. Google will include an identifying mark on Digitized File images served to End Users through Display Uses that use such Digitized File images. In addition, Google will include on all Digitized File images included (1) in an LDC of a Fully Participating Library, and (2) in a Research Corpus of a Host Site, or of Google, to the extent Google becomes an additional Host Site pursuant to Section 7.2(d)(ii) of the Amended Settlement Agreement, information, in the form of a metadata tag or similar form of identification, identifying the institution to which Google provided such Digitized File images. At any time, the Registry, a Fully Participating Library or a Host Site may provide to Google, or Google may otherwise obtain, Digitized File images that may have been obtained due to an Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. With respect to any such Digitized File images, Google will analyze such Digitized File images and provide the Registry with information and results of any such analysis. Information provided to the Registry will include, if determinable, the potential source of such images (*i.e.*, whether such images originated from a revenue model authorized

under the Amended Settlement Agreement or an internal file of Google, a Participating Library or a Host Site).

Google will include as part of its Security Implementation Plan a description of the processes it will use to identify the source of any Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access that may occur. Such description will include an explanation of Google's processes for responding to any such Unauthorized Access, Prohibited Access or Third Party Unauthorized Access.

3.4.3 Forensic Analysis

In the event of an Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access, the Responsible Party identified as the source of such breach will evaluate and analyze all reasonably determinable information to identify (a) the source of such breach (*i.e.*, to determine whether the source of such breach was internal to the Responsible Party or external, such as caused by a third party), (b) how such breach occurred, and (c) ways to prevent any such Unauthorized Access, Prohibited Access or Third Party Unauthorized Access, as applicable, from reoccurring. Each Responsible Party identified as the source for an Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access will meet and confer with the Registry to provide the status of its evaluation and analysis and, upon the Registry's request, any reasonable reports requested by the Registry.

3.5 Network Security

The requirements under this heading pertain to the controls that limit the Responsible Party's access to the network on which unencrypted Digitized Files are accessible.

3.5.1 Electronic Perimeter

An electronic perimeter is created around systems storing and processing unencrypted Digitized Files as one safeguard against theft. The definition of an electronic perimeter may vary according to the needs of a particular Responsible Party to connect systems and networks to each other.

Systems inside the perimeter are only provided with the ability to communicate with systems outside the perimeter for the purpose of

serving data to End Users and for Remote Access as described in Section 3.5.5.

3.5.2 Network Firewall

Maintain a network barrier that acts as a firewall to prevent unauthorized traffic from reaching systems that store unencrypted Digitized Files.

3.5.3 Device Hardening

Maintain documentation for device hardening of network and computing systems that is consistent with guidelines provided by NIST Section 4.2 of NIST 800-123. Device hardening of network and computing systems should adhere to Section 4.2 of NIST 800-123 (Hardening and Securely Configuring the OS). If, however, a Responsible Party does not adhere to Section 4.2 of NIST 800-123, then it shall implement device hardening of network and computing systems that provides protection equivalent to such standard with respect to protecting the security of the unencrypted Digitized Files and that does not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible Party implements device hardening of network and computing systems that provides such equivalent level of protection, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any difference between the requirements of such standard and the Responsible Party's actual implementation of device hardening, (ii) provide a business justification for each such difference, and (iii) demonstrate that such implementation provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

3.5.4 Network Security Testing

Conduct annual reviews or network vulnerability scans that identify issues that PCI DDS describes as level 3 or higher. Security fixes for identified issues should be addressed as described in Section 3.8.2. Documentation of compliance shall be maintained and acknowledged by the ISR or his/her delegate.

If, however, a Responsible Party does not conduct annual reviews or network vulnerability scans as required by the preceding

paragraph, then it shall conduct network security tests that provide protection equivalent to such reviews or such scans with respect to protecting the security of the unencrypted Digitized Files and that do not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible Party conducts network security tests that provide such equivalent level of protection, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any difference between the requirements of the preceding paragraph and the Responsible Party's actual network security tests, (ii) provide a business justification for each such difference, and (iii) demonstrate that the Responsible Party's network security testing provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

Each Responsible Party will maintain documentation describing the findings of the annual reviews, network vulnerability scans or equivalent protection measures required by this Section, as applicable, as well as records relating to the remediation of identified issues.

3.5.5 Remote Network Access

When Authorized Personnel require System-level Access (as defined above) to systems within the perimeter from outside the perimeter ("Remote Access"), encryption and reasonable authentication mechanisms are used to establish the identity of such Authorized Personnel.

3.5.6 Encryption of Digitized Files

In encrypting Digitized Files, the Responsible Party will use the algorithms and key sizes recommended in NIST SP 800-57 Part 1 – Recommended algorithms and minimum key sizes table. If, however, a Responsible Party does not adhere to NIST SP 800-57 Part 1 – Recommended algorithms and minimum key sizes table, then, in encrypting Digitized Files, it shall use encryption algorithms and key sizes that provide protection equivalent to such standard with respect to protecting the security of the unencrypted Digitized Files and that do not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible

Party uses encryption algorithms and key sizes that provide such equivalent level of protection, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any difference between the requirements of such standard and the Responsible Party's actual encryption of Digitized Files, (ii) provide a business justification for each such difference, and (iii) demonstrate that such implementation provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

Encryption keys will only be provided to Authorized Personnel.

3.6 Media Protection

The requirements under this heading pertain to the Responsible Party's protection of media containing unencrypted Digitized Files.

3.6.1 Media Access

Access to media containing unencrypted Digitized Files must be limited to authorized individuals only.

3.6.2 Media Inventory

Maintain a media inventory log to verify that periodic media inventories are performed. The ISR or his/her delegate should validate that such a log is maintained.

Digital media, such as hard drives and magnetic tape containing unencrypted Digitized Files, is tracked so that theft or loss of unencrypted Digitized Files can be detected. Media will be labeled in a way that facilitates tracking.

3.6.3 Media Storage

Storage media containing unencrypted Digitized Files are maintained on premises or stored off-site in controlled facilities. Only a limited number of Authorized Personnel are authorized to release or receive tapes containing unencrypted Digitized Files (backup media) from an offsite storage vendor. Documentation of the list of such personnel is maintained and reviewed periodically, but no less frequently than annually, by the ISR or his/her delegate.

3.6.4 Media Sanitization and Disposal

When digital media are retired or replaced, any Digitized Files that are unencrypted will be deleted or rendered permanently unusable from the digital media.

Maintain an “end of life” disposal process for all media hardware components. Disposal of media that contains unencrypted Digitized Files must render the data unrecoverable. This requirement includes, but is not limited to, magnetic tape, CD-ROM, DVD, hard drives, and USB devices.

3.7 Physical and Environmental Protection

The requirements under this heading pertain to the Responsible Party’s safeguards with respect to physical access to and protection of Digitized Files that are unencrypted.

If, however, a Responsible Party does not adhere to these physical access safeguards with respect to its scanning facilities, then, with respect to such facilities, it shall implement safeguards that provide protection equivalent to the requirements of this Section with respect to protecting the security of the unencrypted Digitized Files and that do not pose an undue risk of a security breach that would result in Unauthorized Access, Prohibited Access or Third-Party Unauthorized Access. If the Responsible Party implements physical access safeguards that provide such equivalent level of protection for its scanning facilities, then, in its Security Implementation Plan, the Responsible Party shall (i) describe any difference between the requirements of this Section and the Responsible Party’s actual safeguards, (ii) provide a business justification for each such difference, and (iii) demonstrate that such implementation provides such an equivalent level of protection and does not pose any such undue risk of a security breach.

3.7.1 Physical Access Authorizations

As a safeguard against physical theft, access to facilities where unencrypted Digitized Files are stored or processed is restricted. The level of access varies and depends on the role of the Authorized Personnel accessing such unencrypted Digitized Files and whether such Authorized Personnel are “trusted agents” or certified third parties.

Access to the Responsible Party's facilities where unencrypted Digitized Files are stored or accessible and similar sensitive areas are restricted to only the Responsible Party's authorized employees, vendors and contractors, certified third parties, and authorized visitors.

Access to sensitive areas where unencrypted Digitized Files are stored or accessed, such as data center(s) and tape libraries, for all persons requires approval by appropriate facilities managers. The approvals are documented. Access for terminated or transfer employees is revoked on or before the last day of employment.

3.7.2 Physical Access Control

The use of entry systems, such as card readers, is used where possible to verify the credentials of Authorized Personnel passing through doors and to provide a method of tracking these individuals.

3.7.3 Visitor Control

Visitors to facilities where unencrypted Digitized Files are kept will be individually authorized for access. Responsible Parties will maintain a process for admitting visitors into areas where unencrypted Digitized Files are kept. This process will include controls on who can authorize access and a detailed description of how visitor log records for the facility are kept.

3.7.4 Access Records

No less than annually, the ISR or his/her delegate shall review the currency and appropriateness of physical access to the facility where unencrypted Digitized Files are stored and sensitive areas. Logs will be maintained so that discrepancies can be discovered.

3.8 Risk Assessment

The requirements under this heading pertain to the auditing and discovery of security vulnerabilities.

3.8.1 Risk Assessment

Pursuant to Section 8.2(c) of the Amended Settlement Agreement, the Responsible Party is required to permit a mutually agreeable

third party to conduct annual (or, if reasonably necessary, semi-annual) audits of security and usage to verify such Responsible Party's compliance with its then-in-effect Security Implementation Plan.

3.8.2 Vulnerability Management

Maintain a program and process to identify newly discovered security vulnerabilities, including as a result of network security testing pursuant to Section 3.5.4. Security fixes (*e.g.*, patches, mitigating controls) are to be applied as soon as possible when vulnerabilities are deemed critical in order to protect the asset from intrusion vulnerabilities.

If, however, a Responsible Party does not or will not apply a security fix as soon as possible when it discovers a vulnerability deemed critical, then, in its Security Implementation Plan and to the auditor the Responsible Party shall (i) provide a business justification for not doing so and (ii) demonstrate that not fixing such vulnerability does not pose any such undue risk of a security breach.

3.9 Digitized File Content Delivery by Google

This Section describes the security requirements applicable to Google in serving the content of Digitized Files to End Users under the terms defined in the Amended Settlement Agreement.

3.9.1 Preview Uses

Google shall use commercially reasonable methods to identify unique Access Points from which Books contained within Google Book Search are being accessed for the purposes of Preview Use through signals such as the IP address, cookies and similar signals that may be available. Google shall monitor and track access to Preview Use pages from unique Access Points. "Access Point" means a specific computer from which Google Book Search is accessed to the extent such access can be identified through signals such as a cookie, IP address or similar signals. Different End Users accessing Google Book Search from the same computer will be tracked as a single End User for the sake of monitoring Preview Uses.

For each unique Access Point, Google will track and count unique Preview Use pages viewed for each individual Book. When the number of Preview Use pages from a specific Book accessed from a single Access Point has reached the allowed Preview Use quota, Google will restrict future access to such Book by that End User from the Access Point to the Preview Use pages that that End User already has viewed.

Google shall identify blacklisted pages for each Book and will use commercially reasonable efforts to prevent those pages from being shown to any End User as part of any Preview Use. Google may change the specific pages that will be blacklisted for a given Book from time to time. Google shall use commercially reasonable efforts to keep blacklisted portions of a Book from changing for a period of at least ninety (90) days.

3.9.2 Consumer Purchase

Google shall use commercially reasonable efforts to authenticate individual End Users purchasing access to individual Books through the use of account login or other equivalent method. An End User that is logged in will be identified as an Identified User based upon such End User's login account information.

Access to the full contents of a Book through Consumer Purchase will be limited to identified End Users who have purchased access to that Book.

Google will encourage End Users to not share or transfer their accounts by monitoring simultaneous login. If Google determines that an identified End User is simultaneously logged in and accessing books from two computers, then Google shall disable one of the Access Points and require re-authentication from that Access Point.

3.9.3 Institutional Subscription

Google shall use commercially reasonable efforts to authenticate individual End Users for access to Books in an Institutional Subscription by verifying that an individual is affiliated with an institution with an active subscription. Google's efforts will be in partnership with the subscribing institutions in a manner consistent with, or otherwise equivalent to, generally accepted industry standards for authentication of use of subscriptions. Techniques

used may include IP address authentication, user login, and/or leveraging authentication systems already in place at an individual institution.

3.10 Access to Research Corpus by Host Sites

A Host Site's Security Implementation Plan shall describe the processes and procedures it will employ to comply with the requirement in Section 7.2(d) of the Amended Settlement Agreement, and in the Host Site-Registry Agreement, that only Qualified Users, reviewers and challengers may have access to the Research Corpus.

3.11 Use of Library Digital Copy by Fully Participating Libraries

A Fully Participating Library's Security Implementation Plan shall describe the processes and procedures it will employ to comply with the requirements in Section 7.2(b) and Section 7.2(c) of the Amended Settlement Agreement, and in the Library-Registry (Fully Participating) Agreement, that permit and prohibit access to that Fully Participating Library's Library Digital Copy.