Security and Privacy Policy

Change Management

All changes must be approved by the VP Product Management, Group CTO or Lyceum CTU (Mads Diermayr, Asger Alstrup Palm or Lars Kirkeskov Sørup) .

If you have any suggestion changes please make revision and ask for approval before it can be considered valid.

Change log:

- 05/15/2019 Mads Diermayr: Version 1.0 initial draft.
- 05/22/2019 Mads Diermayr: Version 1.1 final.
- 09/05/2019 Mads Diermayr: Version 1.2 (Added FOSS Policy).
- 02/11/2019 Mads Diermayr: Version 1.3 Added Open Source tools and technologies.
- 11/12/2019 Mads Diermayr: Version 1.4 Added access lifecycle, IT Risk Assessment and frequency of security scans.
- 01/28/2020 Mads Diermayr: Version 1.5 Added administrative logging information.
- 02/19/2020 Lars Sørup: Version 1.6 Added security scan definition/access control management.
- 03/17/2020 Lars Sørup: Version 1.7 Risk Management Process added.
- 03/17/2020 Lars Sørup: Version 1.8 Vulnerability scanning text update.
- 04/03/2020 Lars Sørup: Version 1.9 Vulnerability scanning upgrade of frequency and scope.
- 04/04/2020 Lars Sørup: Version 1.10 Moved section and further vulnerability scanning updates.
- 05/27/2020 Mads Diermayr: Version 1.11 Added Firewall Policies.
- 07/15/2020 Lars Sørup: Version 1.12 Scanning Policy Updated (vendor entered and added a precision on the base image).
- 03/08/2020 Mads Diermayr: Version 1.13 FERPA, PPRA, COPPA.
- 11/26/2020 Mads Diermayr. Version 1.14 updated architecture diagram.
- 12/16/2020 Mads Diermayr. Version 1.15 added information about multi tenants.
- 12/17/2020 Mads Diermayr. Version 1.16. Updated Risk Management section. Updated Cloud security section. Updated Change Management section.
- 12/21/2020. Mads Diermayr. Version 1.17. Updated Privileged access lifecycle system quality process management procedure section, Updated Change Management process.
- 12/22/2020. Mads Diermayr. Version 1.18 Information handling and security.
- 12/23/2020 Lars Sørup. Version 1.19 Not removable medias allowed for computers connection to prod.
- 08/01/2021. Mads Diermayr. Version 1.20 Added Workstation Hardening information and access scope.
- 08/02/2021. Mads Diermayr. Version 1.21 Edited Workstation Hardening information and access scope.
- 09/02/2021. Lars Sørup. Version 1.22 Added Change Management procedure. (Approved by Lars Sørup)
- 12/02/2021. Mads Diermayr. Version 1.23 Updated Workstation Hardening information for Linux Ubuntu (Approved by Mads Diermayr)

Change Management 1

Information Security Policy and Compliance 5

Incident Reporting 5

Overview 5

Workforce Responsibilities 5

Risk Identification and Control Assessment 5

Initial Incident Reports 5

Incident Response Team 6

Risk Management Process 7

Purpose 7

Overview 8

Identification Phase 8

Mitigation and recovery planning 9

Implementation plan 10

Management 10

Security in Human Resources 11

General staff 11

Developer onboarding and training 11

Information Handling and Encryption 12

Storing 12

Sharing 13

Purpose 13

Retention 13

Transparency 13

FERPA, PPRA, COPPA 14

Access Control 14

Privileged access lifecycle system quality process management procedure 14

Production data access 14

End user access and logging 15

Password Policy 15

System and Network Infrastructure 15

Diagram of Production Environment 16

Integration with external systems 16

Data flow for SCORM 16
Data flow for LTI 17
Environments 17
Firewall information and Policies 18

3rd Party Relationships 18
FOSS Policy 18
FOSS tools used in Rhapsode Production 18

Physical and Environmental Controls for Information Processing Facilities 19

Vulnerability Management 19
External assessment 19
Recurring assessments 19
Black Box scans 20
White Box scans 20
Docker Image scans 20
New technologies 20

Disaster Recovery and Business Continuity 21
Defences Against Disasters 21
Defences to Keep the Product in Operation 21
Defences to Protect the Product Pipeline 22

Wireless Network 22

Information Systems Acquisition Development and Maintenance 22

The Area9 Development Life-Cycle 23
Area9 Best Practices 23
Area9 Coding Convention 25
Risk-based, iterative development 25
From idea to deployed feature 25
Change Management Procedure 26
Separation of duties 27

Cloud Security, Data Access and Hardening 27
General high level security model 27
Network monitoring 28
Multi Tenant Information 28
Server side code deployment 28

Scopes of data access **29**
Learners (aka End users/Students) 29
Data Access 29
Access Controls 29
Security policies 30
Educators (aka Instructors/Teachers) 30
Data Access 30
Access Controls + Security Policies 30
Curators (Content Creators) 30
Data Access 30
Access Controls + Security Policies 30
Super Admins (A9L Sr Technical Support) 31
Data Access 31
Access Controls 31
Security Policies 31
System Administrators 31
Data Access 31
Access Controls 32
Security Policies 32

Appendix 1: Workstation Hardening Policy **32**
Hardening controls and evidence 33
Disable automatic login 33
Set a password with your screensaver 36
Turn on your firewall 38
Disable remote access 40
Enable or install antivirus protection tools 41
Enable auto-updates for your operating system. 43
Set up file backups 44
Turn on encryption 44
Set up a password manager 46
Disabling External Media as well as autoplay and autorun 47
Allowed Web Browsers and Email clients 48

Information Security Policy and Compliance

Area9 strives to fulfill our obligations about protecting data trusted to us. We do employ industry standard levels of security to our systems, and apply encryption and other security techniques where applicable to ensure a reasonable protection.

As we are an agile development group with frequent deploys, we do not hold any continuous certification as we do not audit every deployed version. The technology management team has evaluated the cost/ benefit and decided to only run occasional audits to ensure that the platform has not digressed while maintaining a reasonable workload and an ability to react timely. Area9 and the learning platform adhere to the proper requirements for handling PII, and living up to the GDPR requirements within Europe and North America as a Data Processor on behalf of our customers/partners as Data Controller. Upon internal audit, Area9 can confirm that we are eligible for certification if the business need ever arose. Additionally, we follow OWASP recommendations for hardware and software security configurations.

Incident Reporting

Overview

This section provides an overview and guidance for the required process for Area9 Lyceum's (A9's) privacy and data security breach.

Workforce Responsibilities

Every workforce member at A9 has the responsibility to immediately report suspected or known breaches of the privacy or security of restricted information to the Security Officer. All incident reports are to be made as soon as possible after the incident is identified, and with minimum delay.

Risk Identification and Control Assessment

Initial Incident Reports

Workforce member incident reports must include the following incident descriptors when describing the incident to their designated reporting point:

- date and time of incident discovery
- general description of the incident
- systems and/or data at possible risk
- actions they have taken since incident discovery
- their contact information
- any additional relevant information known at the time.

Incident Response Team

All incidents are classified by the IRT. The classification informs those involved of the severity and impact of the incident, and ensures that the incident receives the appropriate level of attention. If the incident was classified before being reported to the IRT, the IRT will re-evaluate the classification based on the information available at that point in time.

The incident classification table below provides several incident factors to assist in proper incident classification. Depending on the nature of the incident, some of the incident criteria represented in the table may not be present in a particular incident. Moreover, if an incident contains characteristics in several different severity columns, the severity of an incident must reflect the highest category. For example: if an incident affects a service that possibly involves personally-identifiable information (medium severity) with a likely definite public impact (high severity), the incident should be classified as high severity. Incident classification is a dynamic process, i.e. severity may change one or more times as incident details emerge over time during the investigation process.

Incident Severity Characteristics	Incident Severity Characteristics		
	Low	Medium	High
Criticality – Application	Internal Systems and Applications	Internal or External Systems and Applications	Internal or External Systems and Applications
Criticality – Infrastructure	No	Limited Scope	Organization-wide impact
Impact – User/System	Affects few people or few systems	Department-wide impact	Organization-wide impact
Impact – Public	None	Potential Impact	Definite Impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures
Encryption	Robust encryption algorithm (e.g., FIPS 140-2 compliant), and key control	Weak algorithm and/or key controls	No encryption, or easily defeated encryption
Resolution Procedures	Available and well defined	Resolution procedure not well-defined, bypass available	No resolution procedures or bypass available
Information Sensitivity	Affects an individual researcher or unit	Affects a School or a small campus	Statewide or National impact
Intellectual Property	Initial datasets	Research working papers and completed datasets	Publishable research
Protected Information (Personally Identifiable Information or Protected Health Information)	None	Possible	Definite

Risk Management Process

Purpose

The risk management process defines the actions and processes for handling IT risk at Area9 Lyceum. The purpose of this is to guide the organization to recognition, impact evaluation, investigations, mitigation and implementation.

Area9 Lyceum applies a general risk guided development model, where the management team for the development organization guides the product development based on a “risk-based iterative development” methodology, see our Security and Privacy policy for more details.

Any or all incidents related to actual risk manifestation has to be reported and managed according to our Incident Reporting above.

This process relates to systemic risk identification and management.

Overview

The standard iterative methodology will be employed with regards to Risk Management as can be seen below:

Identification Phase

The technical project owner TPO (at the time of writing the CTO) is responsible for performing a yearly risk analysis (once every year in the period June 1st-May 31st the following year), and updating the risk analysis report for Area9 Lyceum's main platform(s). It is the responsibility of the TPO to involve other relevant stakeholders.

Scope

At the time of authoring only the Area9 Rhapsode™ platform is governed by the process. The Risk Management process is limited to the production environment and related areas (areas with special and/or preferred contact or influence on the product environment), as the single source of customer data hosting.

Areas
The report needs, at a minimum, to review:

- Complexity and relevance of the technologies involved.
- Team composition.
- Platform and Infrastructure.
- Continuous integration, deployment and testing tools.
- Source code management including code review.

Impact Assessment
Risks should be evaluated, and prioritized based on impact.

The assessment is conducted by considering what the potential adverse consequences could be and for whom.

Example list of impact areas:

- Regulatory lack of compliance
- Customer/Partner loss
- Business Opportunity loss
- Reputation
- Harm to society
- Monetary
- Legal risk

Probability should be rated in 3 categories:

- Low (<1%)
- Medium (1-10%)
- High (>10%)

Mitigation and recovery planning

The purpose of mitigation and recovery plan is to help limit the scope and impact of the breach and to restore the service as soon as possible. This is split in two groups/plans, which can occur simultaneously (e.g. reporting the incident can happen while investigation is still in progress).

Mitigation - containing or preferably stopping the incident.

- Investigation requirements.
- Plan for stopping additional data loss
- How to fix the cause of the breach

Recovery plan

- How to recover/restore data
  - Which backup is safe etc.
- How to recover/restore infrastructure
  - change zone
  - provider
  - hosting platform etc.
- Inform authorities if relevant
- Fulfil potential contractual requirements – when applicable
- Identify other people – internal and external – to notify based on the principle that notifications should be helpful and actionable

Implementation plan

For all risks with higher than low probability and significant (as deemed by management) impact, an implementation plan to reduce risk or impact must be developed and implemented.

The implementation plan should aim at reducing both the probability and the impact, and if possible must reduce the risk to acceptable probability or impact. If, for some reason, this is not possible/viable, the plan must provide a description of why and suggest the acceptable state, which must be approved by the management team.

Implementation of risk management plans should happen within the same year they are identified.

Management

All identified risks are documented in the Risk Management Overview with all relevant plans. Yearly Risk Analysis and major events (e.g. management signoff) will be logged manually in the document.

All actions related to the risk management process will be logged in the history of the Risk Management Overview using Google Docs.

All customers' and partners' incident contact information is stored in our CRM system.

Security in Human Resources

General staff

For Area9 Lyceum Management Org Chart, see https://area9lyceum.com/about/the-team/

All employees are screened by relevant managers and agencies before hiring.

Developer onboarding and training

Part of making sure that the code base is secure is making sure developers are skilled and trained.

To learn the Area9 Software Development Life-Cycle (see section), a programmer must pass through 5 phases:

I. Complete the training program, including setup
II. Fix bug
III. Small Feature
IV. Change existing feature
V. Substantial feature

Phases I-IV typically takes about a month for top programmers. Phase V depends on the size of the feature, but after approximately a month, the programmer should typically have completed a first releasable version of the feature. By that time, we consider him out of training.

V. Substantial feature
By doing this satisfactorily, the programmer will prove he can work with the Area9 Agile Software Development Life-Cycle and can:

- develop in iterations
- review own work
- collaborate with other programmers for help in technical issues (e.g., code review or help in developing)
- collaborate with other stakeholders (for specs or for specific questions about the feature and review of next iteration)
- collaborate with his manager (for same reasons)

- plan own work
- navigate the code and resolve technical issues related to any task in the given code base.

Through all phases, and especially in phase V, the programmer will need to demonstrate ability to understand and follow Area9 Best Practices.

Astronauts
Programmers are prone to making these three mistakes:

1. writing code that is not needed
2. not making the code easy to change
3. being too generic

We combat this by not writing code until it is actually needed. We only generalize code the third time it is needed (although “copy and paste” is never acceptable).

Information Handling and Encryption

All data is encrypted in transit using HTTPS TLS 1.2+.

Storing

Area9 Rhapsode™ does not collect any other personal information from the users than username, email and Password. All other data collected is learning data from the user’s interactions with the system. This data is stored securely.

Optionally, users are able to add a first and second name that the system will use to personalize the interface by showing the first and second names in the menu and taskbar.

The Username and Password can be delivered to Area9 Rhapsode™ through OAUTH or another standard. GDPR requires us to ensure we only show data to those who have permission and clearance to view it. But since we only need a unique identifier, we don’t actually need any personal info at all (even name).

Most often emails are used as usernames. If integration with a customer sign-in solution is used, then we only have what that sign-on solution provides. For us it’s a random sequence of characters.

Only passwords are encrypted at rest in the database using SHA-256+PBKDF2.

Sharing

Area9 Group will not share our data with 3rd parties – that is – we will not sell or in any other way give your data to other providers.

We do use 3rd party tools to keep data, but we have agreements with these vendors about our data that prohibits any 3rd party use.

If you login to an Area9 service using a single sign-on solution, there is of course a sharing of your basic login and contact information between those services, but in that case we do it using industrial standard security.

If required by law to share information about you, we will commit to minimize the sharing to the required level, and we will to the extent permissible tell users that are impacted.

Purpose

Area9 Group stores user data mainly in our technical platforms. These applications store a multitude of user data depending on the purpose of the platform. Each platform will individually describe the actual data stored and the specific purpose.

We also store data about our customers and potential customers. The information we store is contact information, correspondence and logging of interaction. We use this to make sure we keep track of our relationship, and have a corporate memory, e.g. in case an employee leaves one or the other organization, to get in touch with newsletter, notification about new blog entries, and depending on our relationship and if required your consent, contact you with offers etc.

Retention

For each of our software platforms we publish the retention periods in the platform for you to see and understand the lifecycle of your data. For data outside our software platforms e.g. customer relationship data, we store them only for as long as it is legally allowed and it has a meaningful purpose.

This period varies grossly between the types of data, our relationship and legal requirements, so we cannot offer a single time period for all data types.

Transparency

The personal data about you is yours – and we are happy to provide you with a copy of your data on request. We share your interest in the data being up-to-date and are happy to assist with getting

a copy of the data, editing, restricting/changing consent to processing or even deleting the data on your request.

For each of our software platforms we provide contact details for you to request a copy of your date and to request deletion or corrections.

For general requests for information, and for customer relationship data please contact gdpr@area9.dk with data related requests.

FERPA, PPRA, COPPA

Area9 Lyceum will never give data on students to 3rd party companies or use the data in ways not intended without full disclosure. See also section Information Handling and Encryption

Area9 Lyceum does not act or function as a School. Area9 Lyceum will comply with all FERPA, PPRA or COPPA related requests from school entities purchasing or utilizing Area9 Lyceum's Software tool regarding proper handling, deletion or extraction of data. (https://www.studentprivacymatters.org/ferpa_ppra_coppa/)

Access Control

Privileged access lifecycle system quality process management procedure

Any staff changes at Area9 Lyceum™ to the defined and named personnel with access to critical data, must undergo a review, audit and approval process by our CTO and CEO.
The list of admin access accounts is reviewed on a yearly basis before the end of Q2.

Access to web servers is restricted to relevant ports only. SSH is firewalled to a restricted set of IP addresses. All access attempts by administrative personnel are logged using Linux built in tools. -All actions performed in the production environment will be logged by MySQL Audit and Linux Audit Tools and will be stored off system using AWS Services.
Admin logs and actions are reviewed yearly before the end of Q2.

Production data access

See Cloud Security section

End user access and logging

All user transactions will upon authentication requiring username and password, be assigned with a unique session token. This token grants access only to content and functionality authorized for that user. The token will expire when not in use.

We log all authentication attempts, failed or successful.

Password Policy

End users of Area9 Lyceum Rhapsode must have a password to access the system. There are currently no restrictions on the complexity of the system.

The three key internal Area9 employees with administration access to production servers, follow best practices with strong, randomly generated passwords, see Cloud Security and Hardening section below.

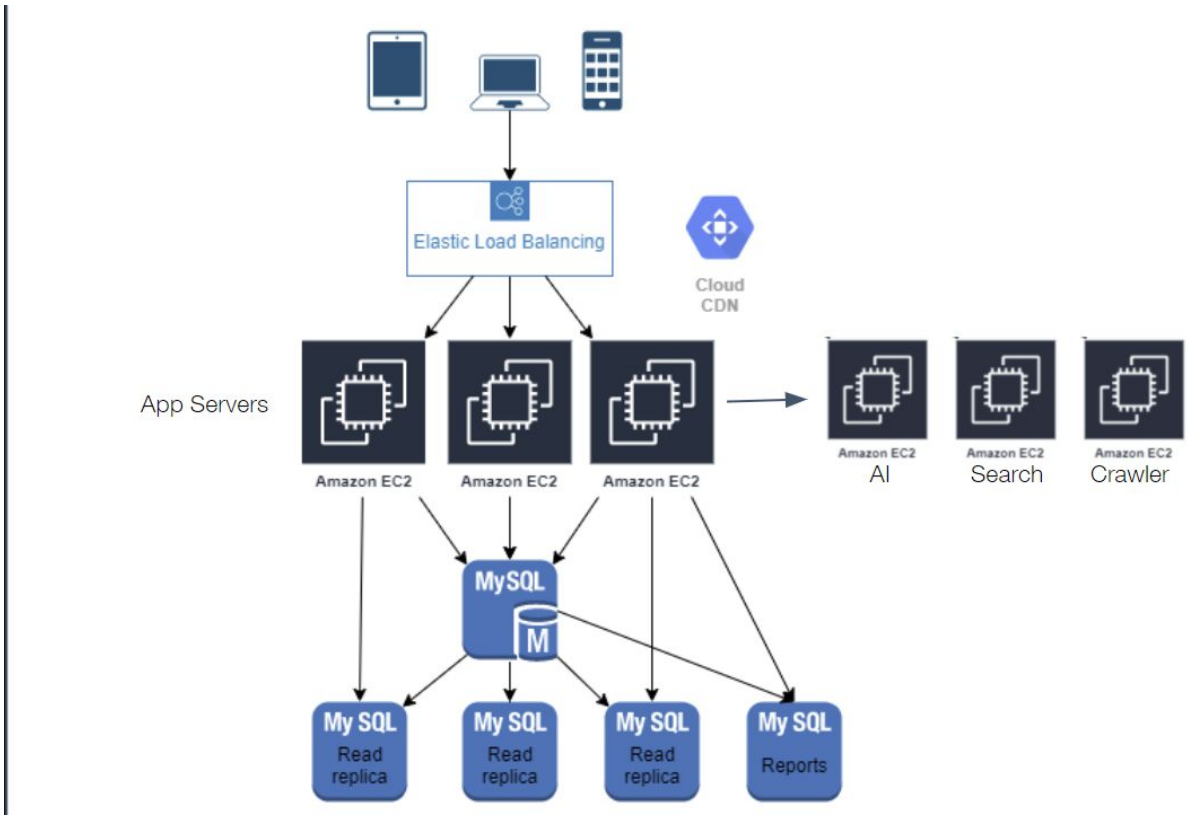
Exemptions: Customers integrating with our systems using SSO are responsible for user credentials and passwords

System and Network Infrastructure

Area9 production systems are completely separated from other infrastructure and are running in AWS. Currently we have instances running in these regions:

- Northern Germany (EU)
- US-East1 - Virginia

Diagram of Production Environment



DB: Mysql 8.x
App Servers: Apache 2.3
Protocol: HTTPS TLS 1.2+
Encryption at rest: Passwords are encrypted at rest with SHA-256+PBKDF2

Integration with external systems

Rhapsode optionally integrates with external systems using OpenID for SSO or Scorm and LTI to integrate with external LMS.

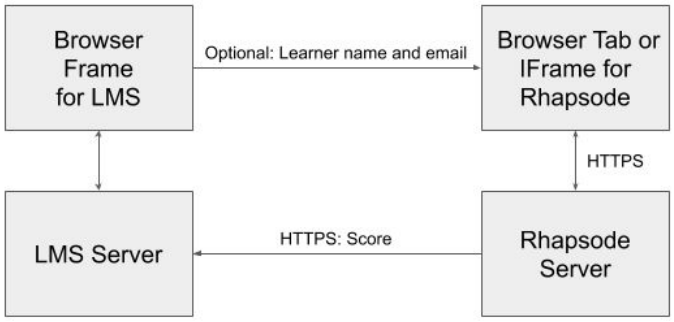
Data flow for SCORM

For SCORM all data communication is done via the Browser. The LMS will launch the SCORM package in an IFrame, the LMS Frame and Rhapsode IFrame are communicating via

Javascript. The LMS will make various identifiers available to the Rhapsode IFrame. In addition the LMS can make the Learner name and email available to Rhapsode. Rhapsode does not require the Name and Email, and it is possible to configure Rhapsode not to collect this information. The Rhapsode IFrame will communicate with the Rhapsode Server via HTTPS. The Learner authentication (password) is only done in the LMS.

Data flow for LTI

For LTI the initial communication is done via the Browser. The LMS might choose to open Rhapsode in an IFrame or in a Tab. The LMS with make various identifiers available to the Rhapsode IFrame or Tab. In addition the LMS can make the Learner name and email available to Rhapsode. Rhapsode does not require the Name and Email, and it is possible to configure Rhapsode not to collect this information.
If the LMS have an LTI Outcome service, then Rhapsode can report back the score. This is done via a Server to Server HTTPS request.
The Learner authentication (password) is only done in the LMS.



Environments

Area9 Lyceum operated with these environments:

1. Dev
   This is our Continuous Integration environment and does not contain any production data.
2. QA
   Full copy of production environment and data used for testing release branches. All access controls as described above, are in place.
3. Production
   All access controls as described above, are in place.

All the environments are fully separated. Only approved individuals according to the Access Control section have access to the AWS environment and to copy and backup the production DB.

Firewall information and Policies

Firewalls are set with AWS Security Groups and not on individual servers. Firewall rules are reviewed and updated as needed every time a service is added or removed to the group.

3rd Party Relationships

Area9 Lyceum stores data using 3rd party data processors. Area9 has signed agreements with the vendors to ensure they ensure at least the same level of privacy. For exporting to 3rd countries (outside the European Union) we only utilize providers in countries approved to handle Personal Identifiable Data and/or that fulfill privacy shield obligations.
The actual 3rd party data processors will be described in detail on the consent pages of each of our websites and in data processing agreements.

FOSS Policy

Area9 Lyceum complies with the licenses governing its use of any software subject to one or more licenses that meet the open source definition published at OpenSource.org or the Free Software Definition or similar license within the Subscription Services or Deliverables.

Area9 Lyceum employees are not permitted to utilize any Open Source in the production environment without explicit permission.

FOSS tools used in Rhapsode Production

Flow 2019	Docker	C++
PHP 7.x	Git	JS
MySQL 5.7.23	Python	QT

Ubuntu 16.04.6 / 18.04.2 Apache 2.x	Jenkins Haxe / Neko	Java

Physical and Environmental Controls for Information Processing Facilities

All production infrastructure is kept in AWS. See Cloud Security

Vulnerability Management

Area9 performs a secure code review at least annually. The workstations of the entrusted employees with access to the servers are under special scrutiny and measures see Cloud Security section. Code is managed and deployed automatically by CI tools. We do apply critical updates to the servers as needed on at least a monthly basis, but more often if needed.

External assessment

To prevent and detect potential security flaws in the developed code, we adhere to OWASP level 1 and routinely do verification towards it. Given how frequently we release new versions of the software we would be re-certifying against SOC 2 (and ISO) all that time and that would take longer than the releases themselves.

Area9 Lyceum does not object to penetration testing by partners as long as this is planned ahead of time and that Area9 Lyceum can specify which environment is subjected.

Recurring assessments

Area9 performs scanning at 3 levels:

Black Box scans

On or before April 30th 2020 Area9 will scan the platform weekly using Rapid7 insightAppSec web scanning tool. The devops team must report any non-remediated regressions of medium or higher criticality to the management within 2 workdays.

The scan reports will be stored for the last 10 consecutive scans.

Any non-remediated findings accepted by the CTO or Group CTO must be recorded in the scan report that can be presented to 3rd parties (regulatory bodies, customers or partners) on request.

White Box scans

On or before April 30th 2020 Area9 will perform assessments using OpenSCAP by RedHat weekly. This scan has to be run on the server instances of the production system.

Using a tool with credentialled access does yield a significant number of smaller and/or issues with available patches. The Area9 devops team will prepare statistics for all non-significant issues (medium or lower in our tool) to the management on a quarterly basis, while high criticality issues (or above) must be reported within 48 hours if not remediated already.

Any non-remediated high criticality findings must be accepted by the CTO or group CTO and must be recordes in the scan report that can be presented to 3rd parties (regulatory bodies, customers or partners) on request.

Docker Image scans

All base images must be scanned prior to deployment to the production system through the Amazon ECR from May 15th 2020. The scanning reports should be stored and available for the last 10 consecutive deployments.

Any issue of level high or above must be remediated before deployment unless approved by the CTO of the group or Area9 Lyceum and recorded in the scan report that can be presented to 3rd parties (regulatory bodies, customers or partners) on request.

New technologies

If Area9 employs new alternative virtualization technologies or platforms, this Security and Privacy Policy must be updated to ensure a similar level of security can be achieved through proper evaluation of these on a frequency that matches the above.

The Group CTO and the CTO of Area9 Lyceum will review the report Quarterly and decide on the list of issues to be closed, and timelines. This will be added to the general development pipeline.

Disaster Recovery and Business Continuity

All vital production systems have redundancy setups. We have no in-house servers or data centers. All vital files and resources are duplicated and separated across different servers. In the case of an emergency, we have a set of monitoring services that notify us when there are problems. Any emergency response is coordinated within a dedicated Skype group chat, where all key people are included, including our third party DBA from Amazon. All personnel are educated to respond immediately as required. In addition to this, we have a shared DropBox folder that is kept up to date with the latest instructions on how to handle emergencies. It contains detailed instructions for how to diagnose problems, recover from previously identified problems, as well as how to handle unforeseen problems. It also contains contact information phone numbers for all key employees. We regularly practice our response to emergencies, as well as do post-mortem on them to try prevent similar situations to occur in the future. We employ automatic build systems with unit testing on the code repository to make sure all code is safe for deployment.

Defences Against Disasters

We have multiple layers of defense to protect us against disasters.

Defences to Keep the Product in Operation

- The database is replicated in an automatic fail-over configuration, hosted by Amazon
- The application servers are replicated in an automatic, load-balanced, fail-over configuration, hosted by Amazon
- The Amazon Service Level Agreement is at 99.95%. http://aws.amazon.com/ec2-sla/
- We have automatic 1-minute interval monitoring of all servers with automatic notifications/wakeups to people in 3 different time zones: GMT-1, GMT+1, GMT+8
- We have additional monitoring to ensure that products can physically start in browsers
- The learning products are able to continue operation on the client if the servers disappear while in use. The results will be automatically synchronized to the server on the next login.

Defences to Protect the Product Pipeline

Our developers are hand-picked based on a very hard programming test. Our development model is structured to ensure that all developers know how to safely work with the servers on a daily basis. All source code is checked into a versioning control system, and all commits are explained by the developers. We do continuous integration to protect us against integration problems. We have automated build servers and unit tests for key components that run on every commit. If the tests succeed, the build is published to production. We ensure all critical components in our system are understood by at least 2 people at any given time. We use code reviews to ensure that key changes are double checked. All developers have a proxy of the production systems on their local machine, and test changes there. All tasks are tracked in a task tracking system, organized by priority. The developers are largely self-organized. We have a mix of developers recruited through an outsourcing provider in Russia, as well as developers hired directly. We have a right to buy out the developers from the outsourcing provider to work for us directly at any time, including if they go bankrupt.

Wireless Network

All production systems are placed in AWS and are completely separated from regular employee infrastructure. See more information in the Cloud Security section about policies for accessing production systems through Wireless Network.

Wireless networks, including guest networks used by employees are encrypted

Information Systems Acquisition Development and Maintenance

Area9 Lyceum assesses all systems acquired as to whether such a system live up to privacy and security requirements. Open Source Systems are preferred as they allow code reviews and control over updates, support and additions.

The Area9 Development Life-Cycle

Area9 Best Practices

We use many methods and principles, but the following ones are the most defining:

Agility
We use agile methods, but not Scrum. The key principle is cost/benefit analysis. As circumstance changes, the cost/benefit ratio changes, and thus priorities change. As an organization, you have to be able to adjust to changing priorities instantly.

Develop tools, not products
This is the most important principle of all.
Since good programmers is a critical resource, this helps us scale. It also implies that our programmers get to do tasks that are technically more challenging and interesting than they would if they were developing products directly.

The principle of solving a problem by first developing a tool that enables solving the problem applies not only to products for end users: it applies to all we do (for instance project management, budgeting, cash flow management, accounting, selling, editorial work, and so on). It also applies (perhaps most of all), to the programming itself: We develop tools to help the programmers do their work. The Flow programming language is an example.

Continuous integration – no branches in our code repository
Keeps the cost of integration low and transparent. No build up of a hidden cost. Keeps programmers openly accountable and keeps cause and effect of wrong choices in code clearer. Bugs are found faster and are easier to find.

Continuous deployment of non-critical systems
Gives faster turnaround for all stakeholders (fellow programmers, users, SMEs, etc.). Increases value of feedback (of bug reports, design change requests, user tests, etc.) that it is based on the most current code.

Swiss cheese safety model
Safety comes from a set of safety practices, each an imperfect layer of cheese, but together, the whole decrease the risk that problems can go through holes all the way through. Apply this model consciously to determine what the best intervention is to increase safety.

Depending on the situation it may be stricter procedures or more testing. But it may also be automating testing, self-checking systems, design changes, choices in team composition or technology choices. The wrong response to a safety issue may give a false sense of security and complacency, or worse, even decrease safety.

Traditionally, software development processes come with a relatively fixed set of defenses: Unit tests, code review, QA departments, user tests. Those are fairly general defensive practices that work well to increase quality.
However, as with any kind of risk mitigation, each practice comes with a cost. There is both a direct cost in terms of man hours required to perform them, but also an indirect cost in slowing things down and reducing agility.

For that reason, our layers of defense are different. Instead of having defenses that are costly in terms of man-hours, we try to employ automated technical defenses, educate and empower our developers. We try to make results of errors appear as quickly as possible. So we only require unit tests in areas of code where it is likely that this practice will be a total gain. Similarly, we typically use QA teams for release processes, rather than individual tasks.

Underlying all of this is a belief that the best layer of defense is to get excellent programmers, teach them the technology and system, and let them program with a direct interface to the people that know what the result should be.

Prototyping, Iterative development, Regression testing, Pair programming, code reviews, documentation, but only where the cost/benefit ratio justifies it

Architect also implements
Keep the technical design honest. If an architect is in an ivory tower, he is out of touch with reality; yet someone needs to reconcile the high-level overview with practice. Therefore, ensure that the architect is materially involved in day-to-day implementation.

Start with high-risk
Always address high risk tasks as early as possible, avoid pushing risk into the tail of a project where it can challenge delivery.

User tests and Customer feedback
The key to good usability (user experience design) is knowledge about the customer and humility. UX design experience is good, but must not take the place of trying out the product on a real user. Many glaring usability deficiencies would have been spotted at the very first user test.

Heuristic UI tests
An objective, systematic and easy way to evaluate a user interface when user testing is not easily possible.

Similarly, we drop code or projects just as fast when that is warranted.

Organizational patterns
Several of these principles are *organizational patterns*. See a research-based catalogue in COPLIEN & HARRISON: *Organizational Patterns of Agile Software Development*. New Jersey 2004.

Area9 Coding Convention

What separates good code from bad code? Not beauty. Not following a particular design philosophy or style. Not extensibility. But: Maintainability. Code is easier to maintain if it is easy to read. It is easier to read, if it is simple. Brevity is also a virtue. But brevity at the cost of simplicity is not good. Extensibility is good, but this must not happen at the cost of maintainability or simplicity. A further problem with aiming for extensibility is that it increases the cost of coding it, and the cost is often not recouped, because the code ends up being extended in a way different from the one foreseen (or ends up being scrapped or rewritten altogether). For these reasons, the big focus is on maintainability (and thus readability, simplicity and brevity). Maintainable code is also code of high quality.

Risk-based, iterative development

As recommended by experts in software development, we employ a risk-based approach to software development. We adopt Barry Boehm's spiral model (see http://en.wikipedia.org/wiki/Spiral_model) with very short iteration cycles in the order of days. At any given point in time, we assess what is the biggest risk to the projects, and address the biggest risks first in an iterative process. In many cases, this corresponds to adopting agile principles. However, we never let agile principles trump a risk-based assessment. If a situation calls for plan-based development to best reduce the risks, we adopt that.

From idea to deployed feature

The typical life cycle of a feature in a product begins with the identification of a need from the customers. This does not have to be an explicit request from a customer, but is often the result of identifying a diffuse need, and then iteratively developing prototypes towards solving the problem directly or indirectly.

The first prototypes are typically hand drawn on paper. We employ simple mock-up tests using the paper prototypes in case we are uncertain about the wording or layout of the feature. Once we have some confidence in the design and wording, a graphic designer prepares a cleaned-up, electronic version in the intended graphical skin, and if necessary, a final mock-up test is done using this.

After this, the electronic version is uploaded to our task system along with a description of the task. If this is a key component, the design and description is reviewed by a suitable expert. Once approved, the task is prioritized, and then put into our automatic queue of work.

When a suitable programmer is free to start work on this, he will accept the task and mark it as being “in progress”. Every day the work is committed into our source code repository. When the work is committed, it is automatically tested by our build system, and if all tests pass, immediately deployed to the servers. Then the feature is live under a special link.

Through this special link, stakeholders can review the work in progress and provide continuous feedback.

Once the feature is deemed to be complete, it is reassigned back to stakeholders for a review and testing. If the feature works as intended, the case is closed. If not, appropriate feedback is provided, and the programmer resumes work on it until it has the quality required.

At strategic points in the development of a project, relevant parts of the program are reviewed by real end-users in a controlled environment. We typically pair two end-users with each other, and make them solve specific tasks working together. We observe their dialogue to identify difficult or confusing parts.

We also employ fast, cloud-based user testing services, where we get recorded videos of users testing the products. These are useful to improve the basic usability of the products.

Change Management Procedure

Definition of change: Any change needing updating configuration or software on our production environment.

All requests for changes are stored in our change management tracking system. Each change request has a lifecycle and the status and history is part of the record

All code and assets are stored in an online repository with full history and version control available.

Separation of duties

Area9 Lyceum has the following separation of duties

- Change requests
- Change approvals
- Change implementation
- Change verification

Change requests can come from a variety of sources; Customers, Sr Management, Product Management and Internal Users. The format can be verbal, email, support tickets or other sources depending of origin

Change approvals can be done by Sr Management and Product Managers. Change requests will once approved be documented formally in our change request repository and be assigned priority and due dates. The backlog is regularly updated.

Change implementations are done by developers and code reviews are performed by Technical Team leads.

Change verification is done by Product management and QA

Cloud Security, Data Access and Hardening

Area9 Lyceum Rhapsode is hosted entirely in Amazon Web Services (AWS). Systems are running on fully patched versions of Ubuntu 18+.

General high level security model

As it it not feasible for Area9 Lyceum (A9L) to centrally manage all employee devices due to the nature of the distributed workforce, A9L has opted for a model where all production data and systems are stored in the AWS cloud and therefore completely segregated from regular employees' networks. In order to limit the attack vectors and exposure, only 4 trusted and certified individuals known as System Administrators have direct access to these systems.

As for the access controls in the Rhapsode application running in the AWS cloud as a web application, there is no difference between end users and internal A9L employees. All users must have valid credentials and session tokens to be able to access data. This access must be specifically granted by each organization and can be revoked at any time. Exceptions to this will be described in detail in the Scopes of Data Access section below.

Sub Processors of data are not covered in this document, Information can be found in our DPAs. We currently employ AWS and Percona as Sub Processors.

Network monitoring

AWS Security Groups and VPC Flow Logs are used to monitor and log network traffic utilized for troubleshooting problems and/or detect anomalous activity on the production networks. See https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Multi Tenant Information

Rhapsode is a multi-tenant Cloud SAAS solution hosted in AWS. Rhapsode separates tenants with a server level API where proper access rights and valid tokens are required to retrieve the relevant data.

Access to data within an Organization is controlled with Project Teams.Organisations can split up their data into separate Project Teams if internal separation is required. Users can ONLY see data from Project Teams they have read, write or full rights to. This is true no matter if you are using Rhapsode Stand-Alone user management, LMS or SSO.

All Organizations' data is categorized as Internal, meaning only the Organization's internal users have access to this data and that the organization has full control over who has access at any given time.

Server side code deployment

Area9 has developed technology to generate the server side code from the database schemas. This ensures that all access rights rules are systematically and correctly implemented, and we sidestep all human error issues. We aim to minimize the number of exceptions from this. Any non-generated server side code is subject to peer review from both co-developers and technical management to decrease risk of errors.

Scopes of data access

Area9 Lyceum (A9L) operates with the following groups related to scope of access. See the list below where the highest number means biggest scope and greatest security measures needed:

1. Learners (aka End users/Students)
2. Educators (aka Instructors/Teachers)
3. Content Creators (Curators)
4. Super Admins (A9L Sr Technical Support)
5. System Administrators

Each group has different scope and needs for accessessing data in Rhapsode differently and thus have distinct access and security controls.

Another dimension of scope is the individual instances of Rhapsode running in different AWS regions. Due to differences in privacy laws globally, we grant unique access to each individual region based on needs, i.e. an individual with access rights in one region, does not automatically have access to other regions. As an example only EU citizens can have super admin access to our GDPR compliant instance in Frankfurt, Germany.

Learners (aka End users/Students)

Data Access

Learners only have access to their own data and results.

Certain types of content allows peer review of submitted answers, this is managed by the Educator.

Access Controls

End users can access Rhapsode either directly as a web application or through integration with an LMS (using SCORM or LTI) or SSO using Open ID connect.

Rhapsode does not enforce password length or expiration. If this is desired, integration through SSO or LMS is required, meaning customers are responsible for enforcing this.

Rhapsode does not automatically disable accounts or delete accounts. If desired this can be requested or done through a REST API.

Security policies

No other security policies are in place for Learners.

Educators (aka Instructors/Teachers)

Data Access

Educators have access to all of their Learners' data related to the classes they administrate. It is possible to share classes with other Educators anonymously.

It is also possible to integrate anonymously with LMS or SSO meaning students' data will also be anonymous to the Educator in Rhapsode.

Educators also have access to the learning material for which they have been granted access, either in Curator or by other Educators. This is the material they can assign to their Learners

Access Controls + Security Policies

Same as Learners

Curators (Content Creators)

Data Access

When setting up a new organisation in Rhapsode Curator, a main project is created and a user from the organisation is designated as the head Curator. Curators have access to the projects they have been granted Read or Write access to. These rights can be changed at any time by the head Curator.

Curators can

- see all content created in the projects they have access to
- not see any Learner/end user data
- See analytics about content usage

Access Controls + Security Policies

Same as Learners, except no Scorm or LTI integration is possible.

Super Admins (A9L Sr Technical Support)

A9L gives super admin access to the Rhapsode Platform Sr. Technical Support staff. This is needed for expediting troubleshooting of platform issues, technical problems and to help sort out customer support inquiries.

Data Access

Users with Super Admin privileges are able to access all users, projects, content and classes in the Rhapsode Web application. They do not have direct access to the platform database or production systems.

Access Controls

- SSO Two-Factor authentication needed for logging on to Rhapsode. Using G Suite SSO
- Passwords must be 8 characters or longer
- Passwords do not expire unless compromised
- Accounts are blocked after 3 failed attempts

Security Policies

- The list of approved users is reviewed annually
- Must not share account information
- Additions to the list of Super admins must be approved by the Platform and Group CTOs
- Must access Rhapsode using Hardened Workstations, see details Appendix 1: Workstation Hardening.
- When handling user data:
    - Must only view a user's data when explicitly prompted by this user or their administrator
    - Must not share or save any user's data unless permitted by user
- Must not use removable media on Hardened Workstation.
- Requires passing an annual privacy and security training course.
- Must not use wireless networks to access Rhapsode unless through approved VPN solution. This solution is StrongVPN.

System Administrators

Data Access

- Full access to AWS portal

- Full access to Databases
- Full access to Rhapsode Web Application

Access Controls

Same as Super Admins + the following:

- AWS:
    - Must use two-factor authentication. Authentication app on mobile device.
- Uses SSH keys and passwords when accessing Databases
- Must use randomly generated pass phrases stored in password manager
- Workstations have disabled external media storage on workstations by default

Security Policies

Same as Super admins + the following:

- ONLY Windows 10 + Ubuntu 20.x Operating systems allowed
- Must use KeePass for storing keys and passwords with two-factor authentication. Each individual stores their own password database
- Must not use wireless networks to access AWS console or Production systems unless through approved VPN solution. This solution is StrongVPN.
- External storage is prohibited from use, except in these circumstances
    - Exception A: A USB security token is required for accessing AWS console. This device does not have any available storage.
    - Exception B: Transfer of files not suitable for online/cloud transfer can be done on an approved Secure Encrypted USB device. This device must be a Kingston DataTraveler Vault Privacy 3.0.

Appendix 1: Workstation Hardening Policy

- All individuals with access to production systems will be provided with approved company issued hardened workstations. Approved Operating systems are Windows 10.x, Ubuntu 20.x all must be fully updated to the latest version.
- All individuals with super admin rights to the Rhapsode Platform will be provided with approved company issued hardened workstations. Approved Operating systems are Windows 10.x, MacOS 11.x, Ubuntu 20.x all must be fully updated to the latest version.
- It is prohibited to access production servers by SSH, AWS Console or Rhapsode using super admin credentials from any other workstation than the company issued hardened workstation.

- It is prohibited to use any removable media on these workstations, including connecting to mobile devices. See exception under “System Administrator”
- It is prohibited to change ANY hardening settings
- Approved Browsers and Email clients are:
    - Latest 2 versions of Chrome. Must be logged in with personal Area9 G Suite account
    - Gmail latest version (served through Chrome using G Suite)

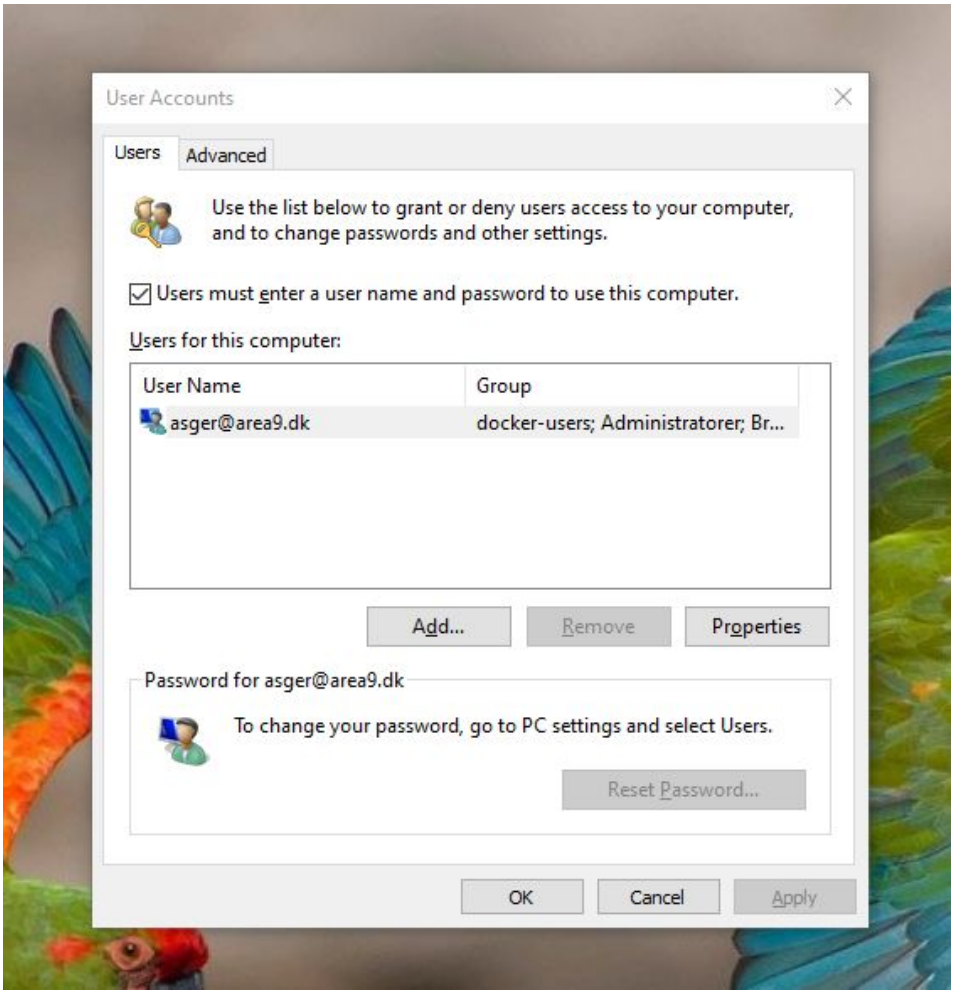
Hardening controls and evidence

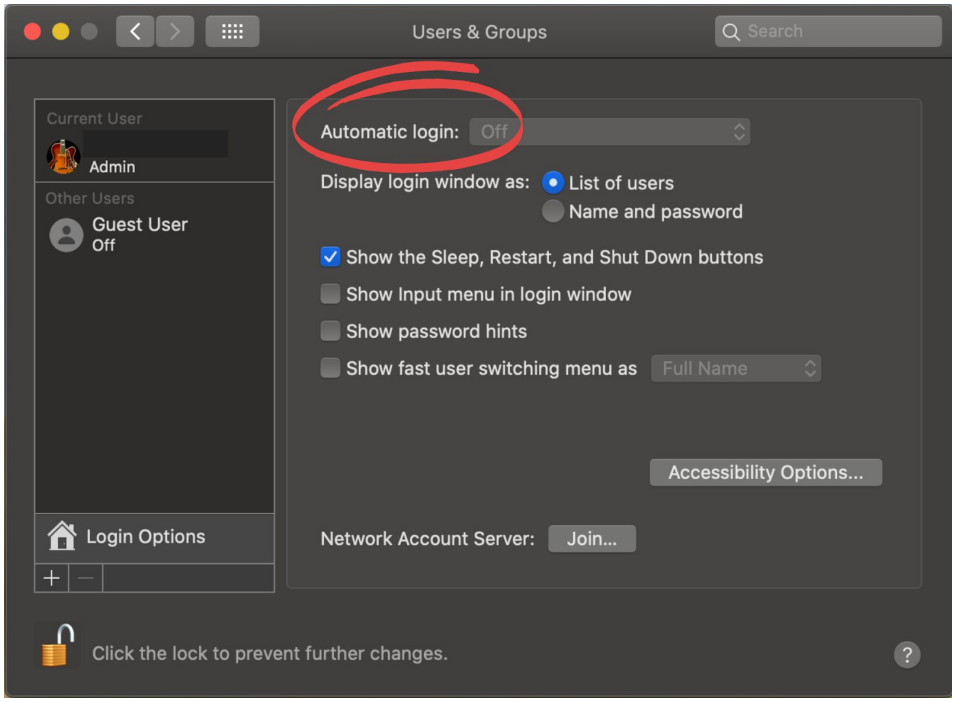
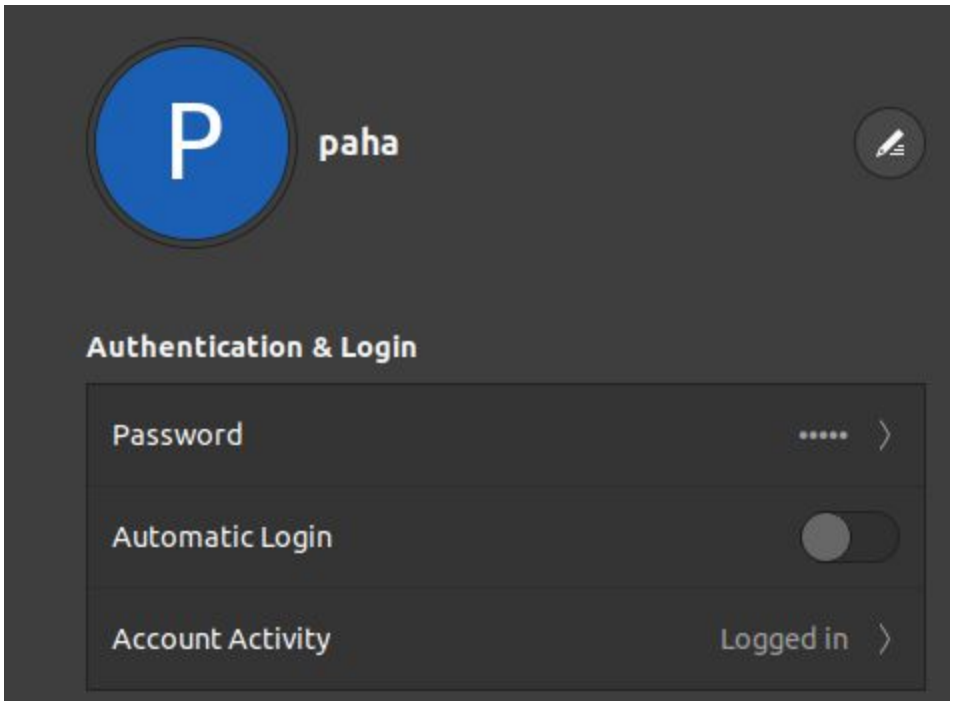
The following shows the different levels of hardening done to workstations accessing sensitive systems. For each section, a sample screenshot is provided for each OS where applicable.

Disable automatic login

Users must not automatically log in to hardened workstations.

OS	Screenshot

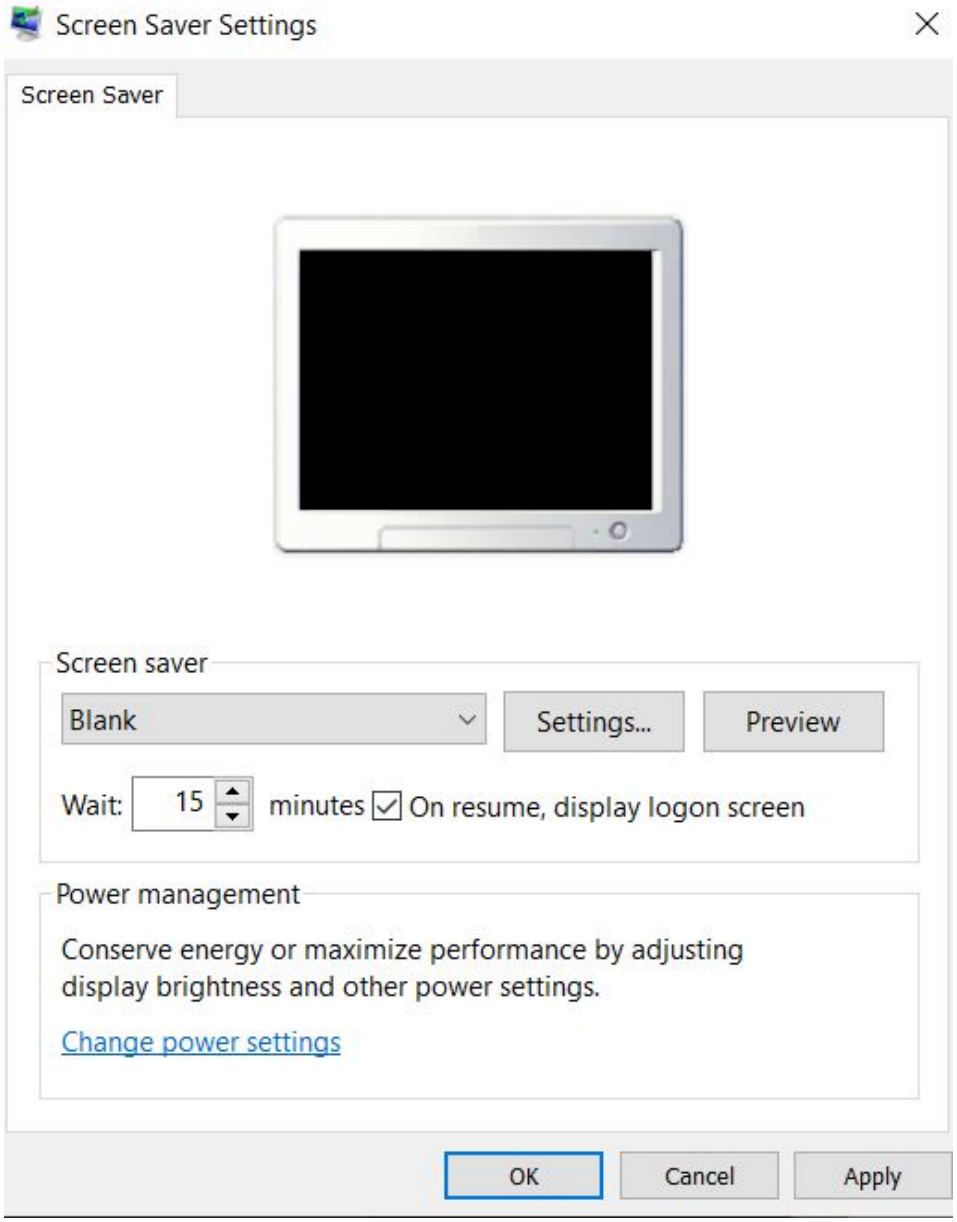
Windows 10.x	

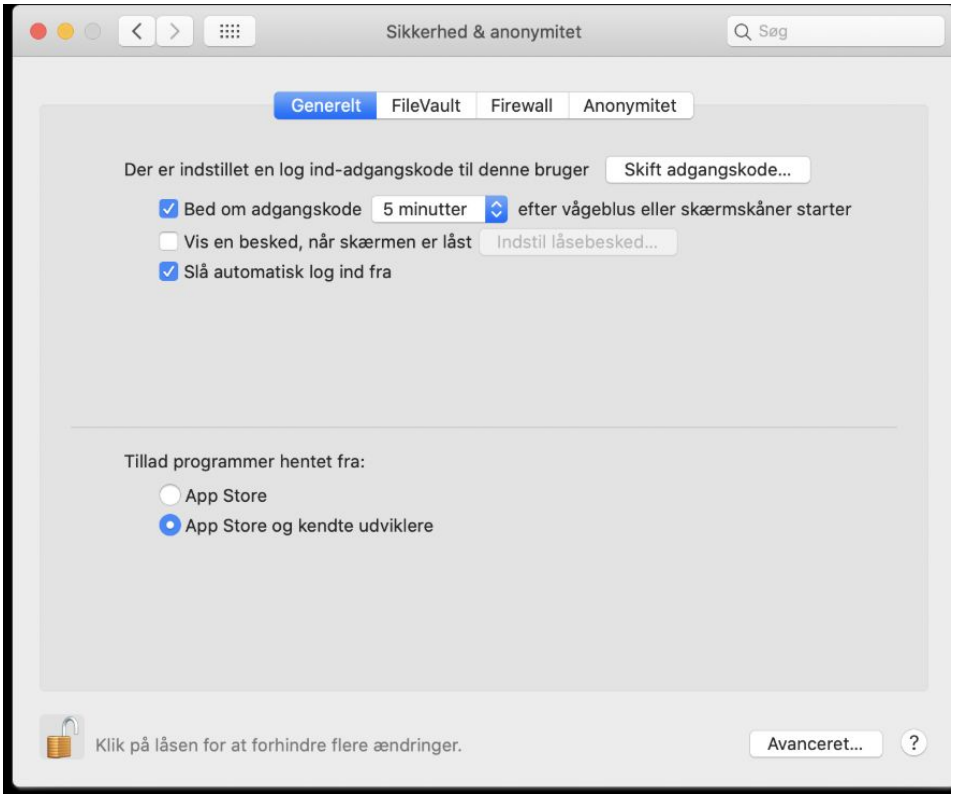
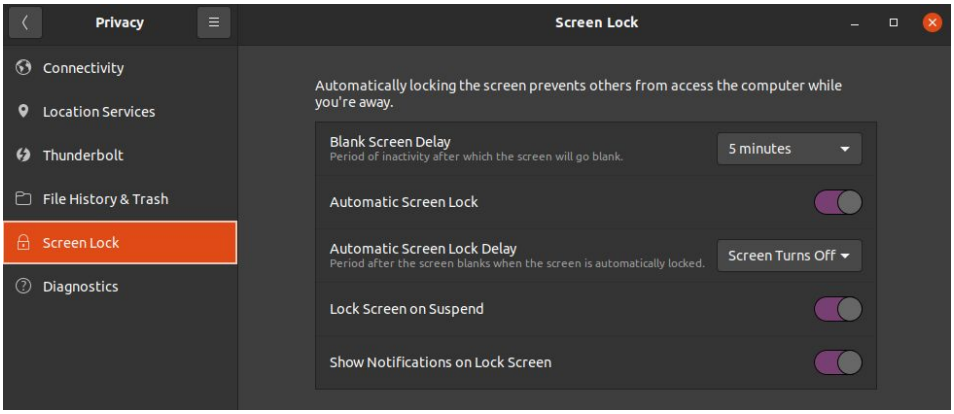
MacOS 11.x	
Ubuntu 20.x	

Set a password with your screensaver

To ensure workstations are not accidentally left open, it must automatically lock after 15 minutes or less.

OS	Screenshot

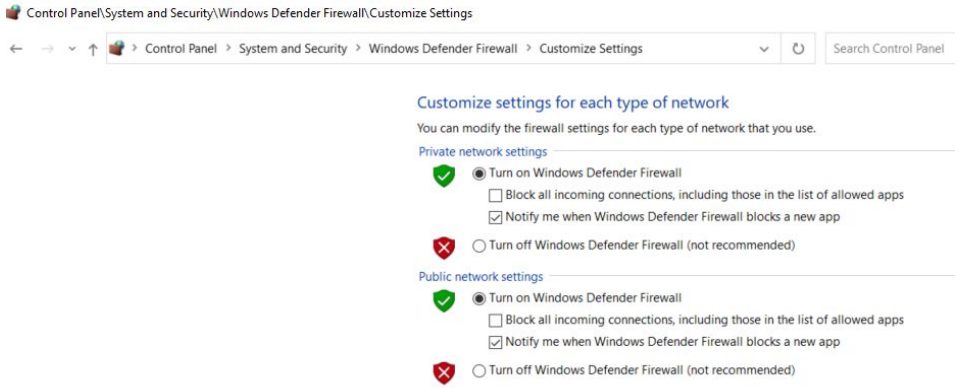
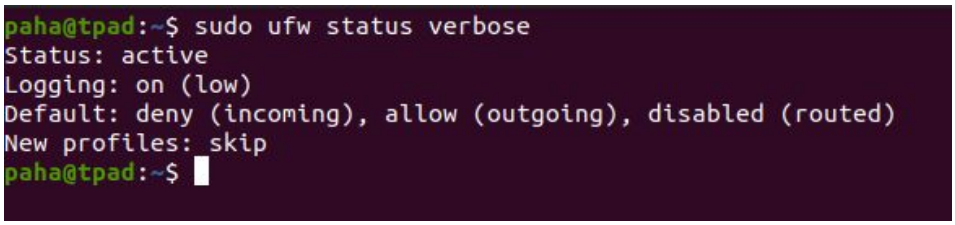
Windows 10.x	
MacOS 11.x	

	
Ubuntu 20.x	

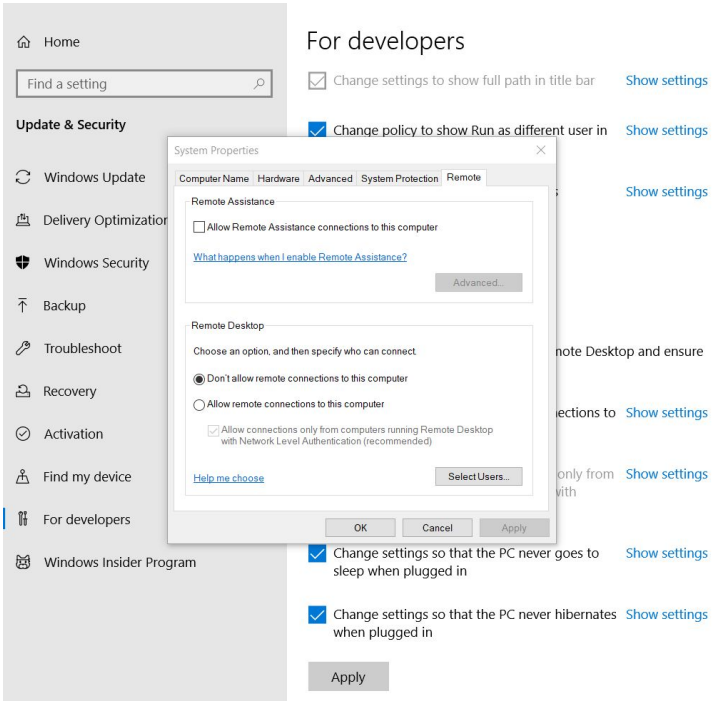
Turn on your firewall

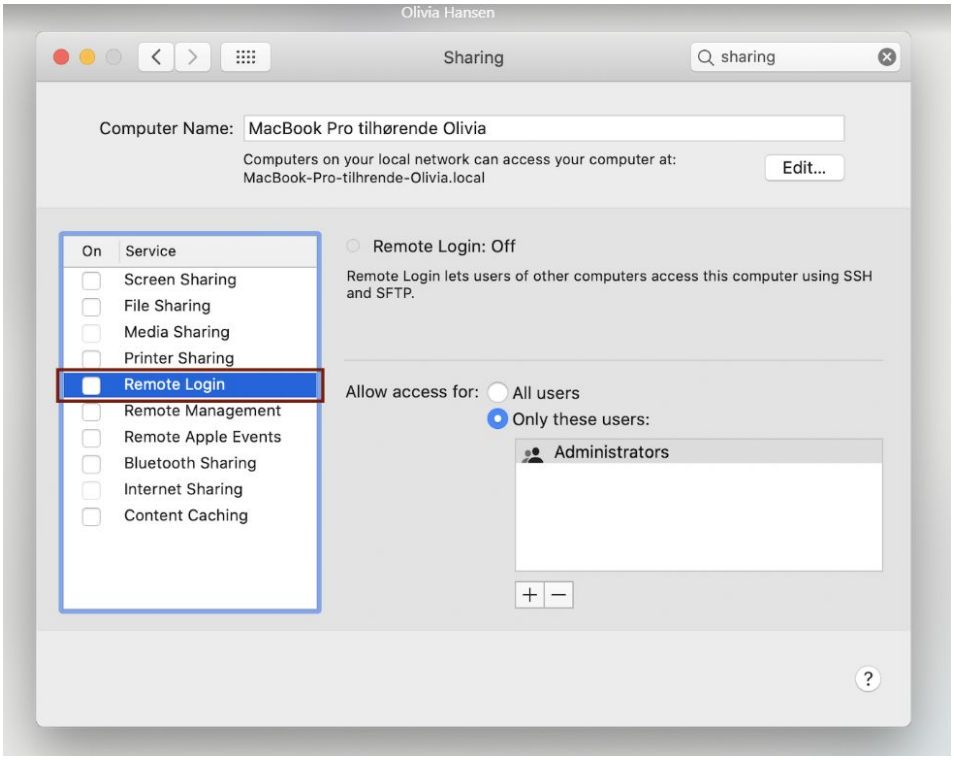
Firewalls must be up to date and running to prevent direct exposure to the network

OS	Screenshot

Windows 10.x Approved Firewall is Microsoft Defender	
MacOS 11.x	
Ubuntu 20.x	

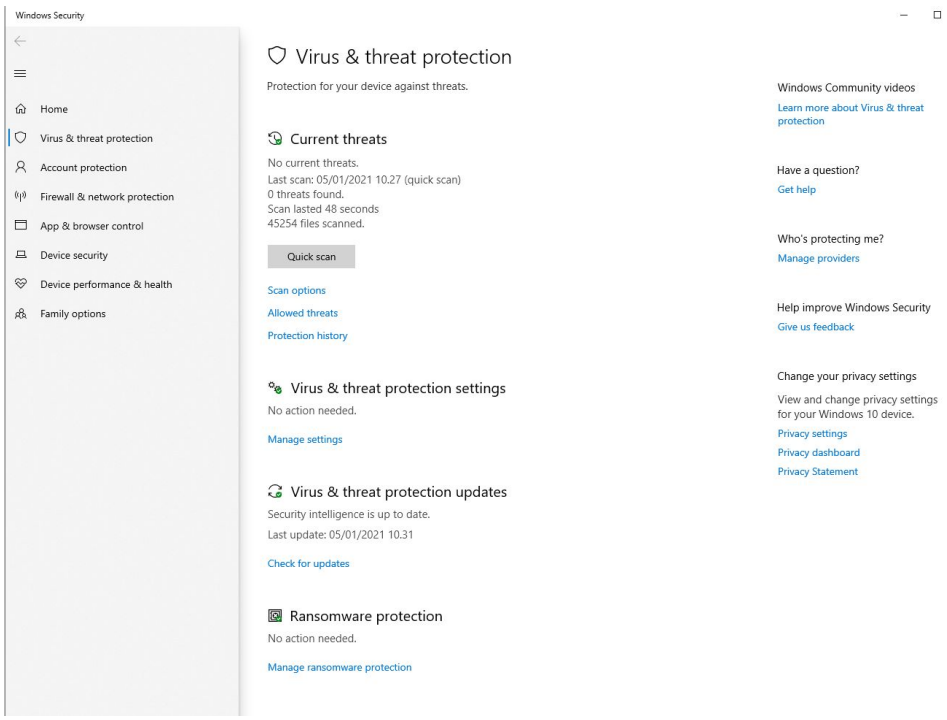
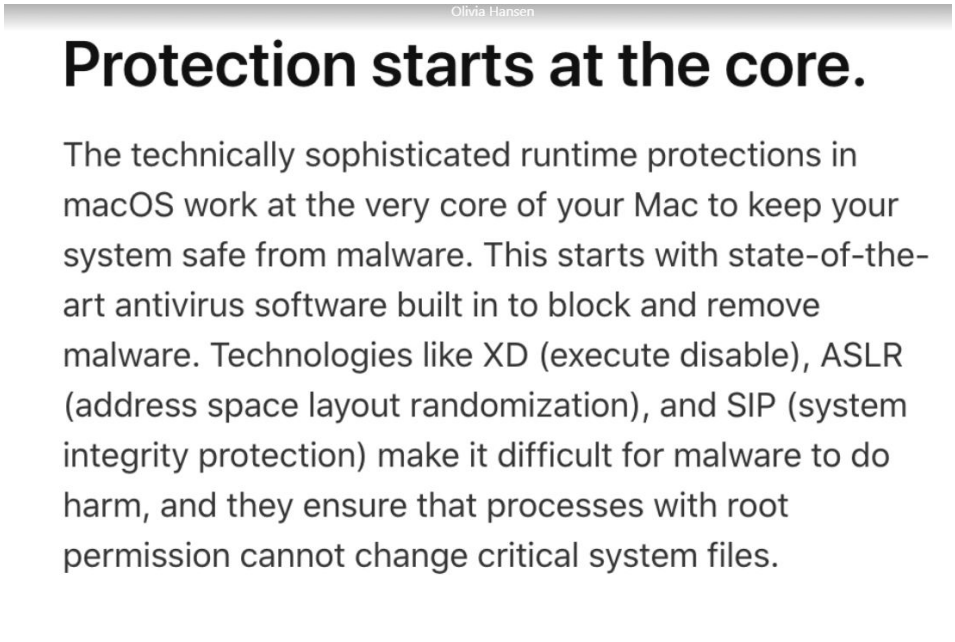
Disable remote access

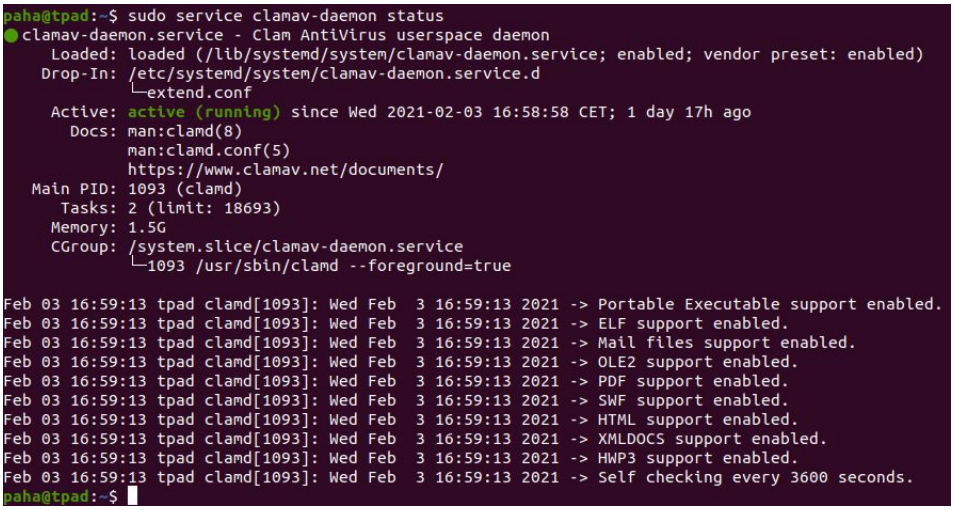
OS	Screenshot
Windows 10.x	

MacOS 11.x	
Ubuntu 20.x	Not yet officially implemented. Expected in place February 2021

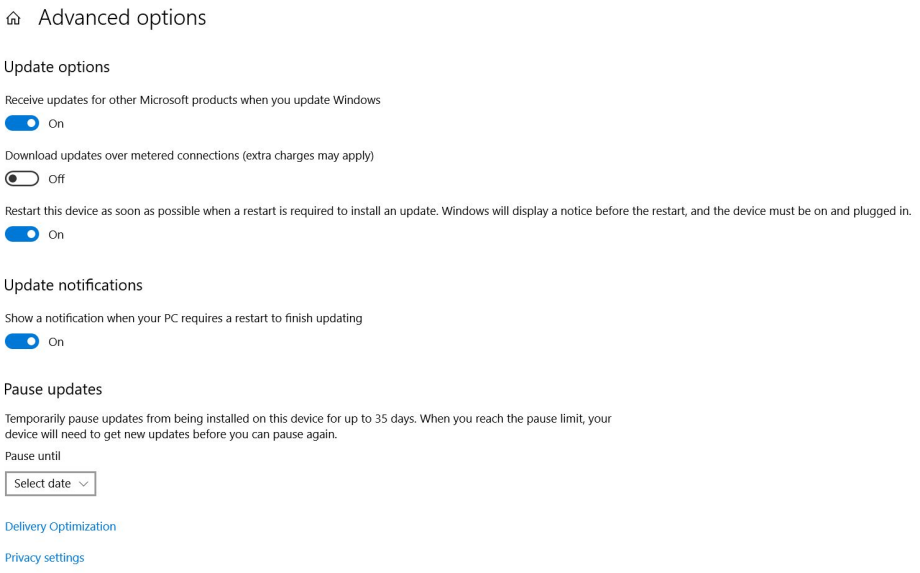
Enable or install antivirus protection tools

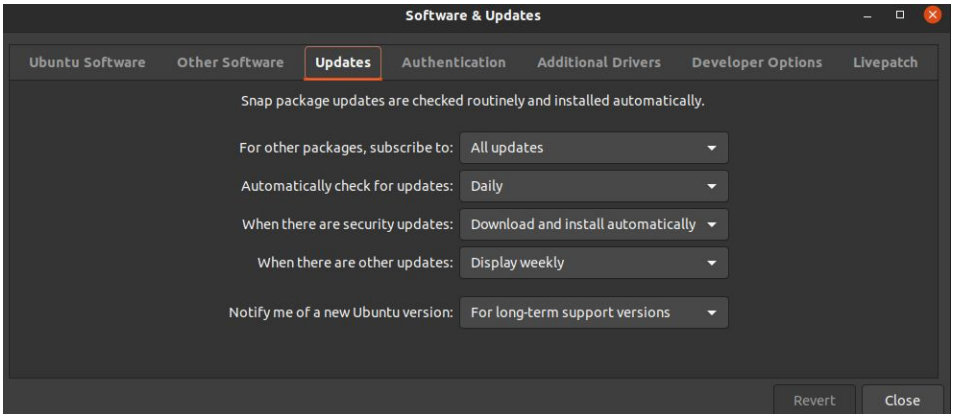
OS	Screenshot

Windows 10.x. Approved Antivirus is Microsoft Defender	
MacOS 11.x	

Ubuntu 20.x	

Enable auto-updates for your operating system.

OS	Screenshot
Windows 10.x	

MacOS 11.x	
Ubuntu 20.x	

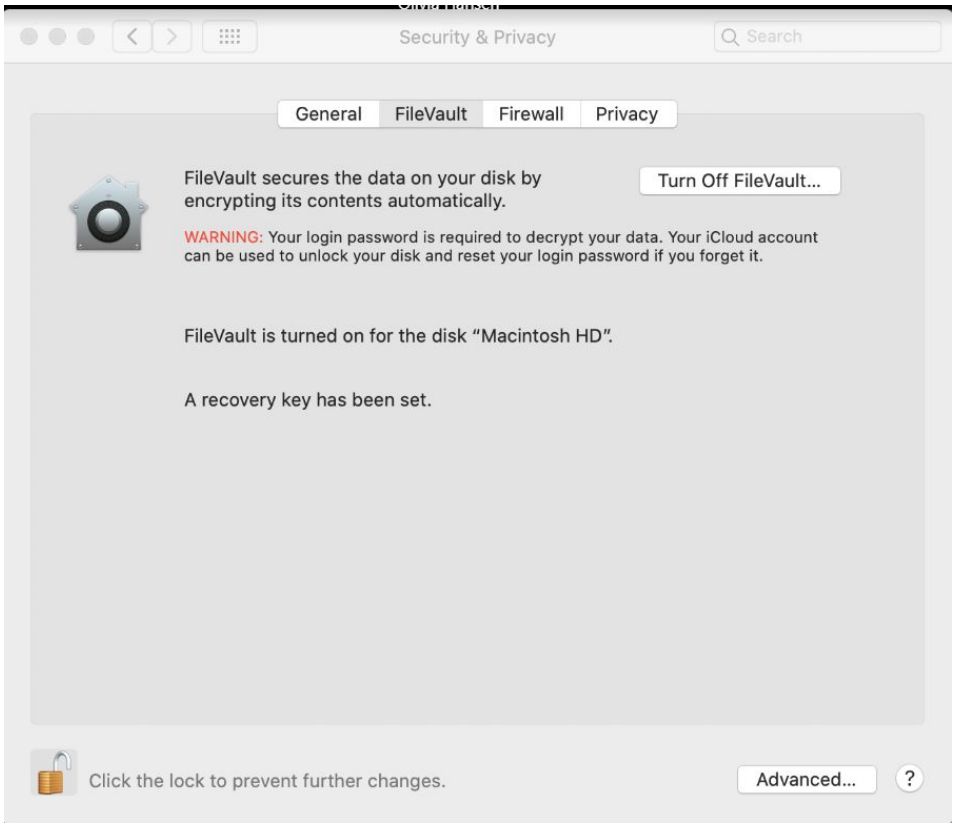
Set up file backups

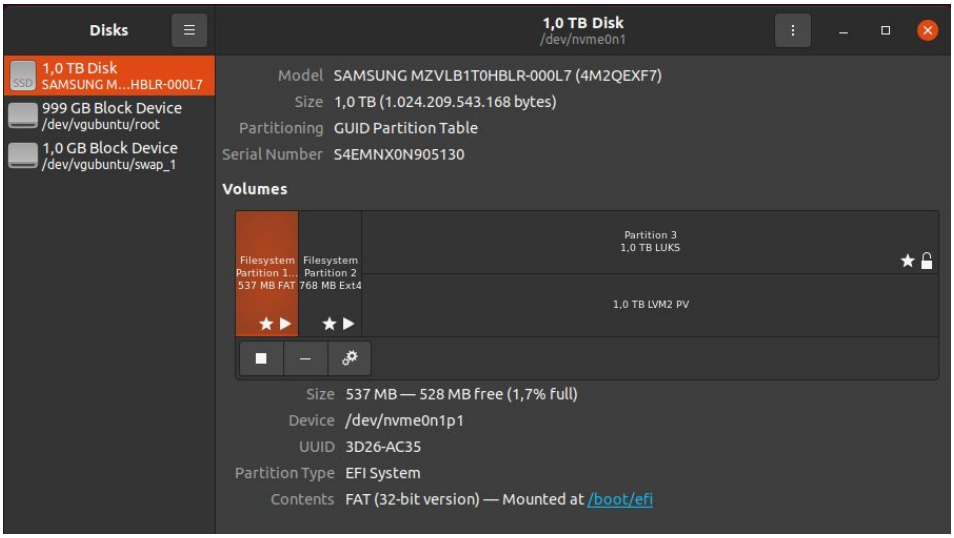
All essential files are stored in online repositories or document management systems:
-Google Enterprise
-Gitea (Internally installed and managed code repository)
-GitHub (Web application for public open source code)
-DropBox

The exception is the password manager file. If lost, all passwords must be recreated.

Turn on encryption

OS	Screenshot

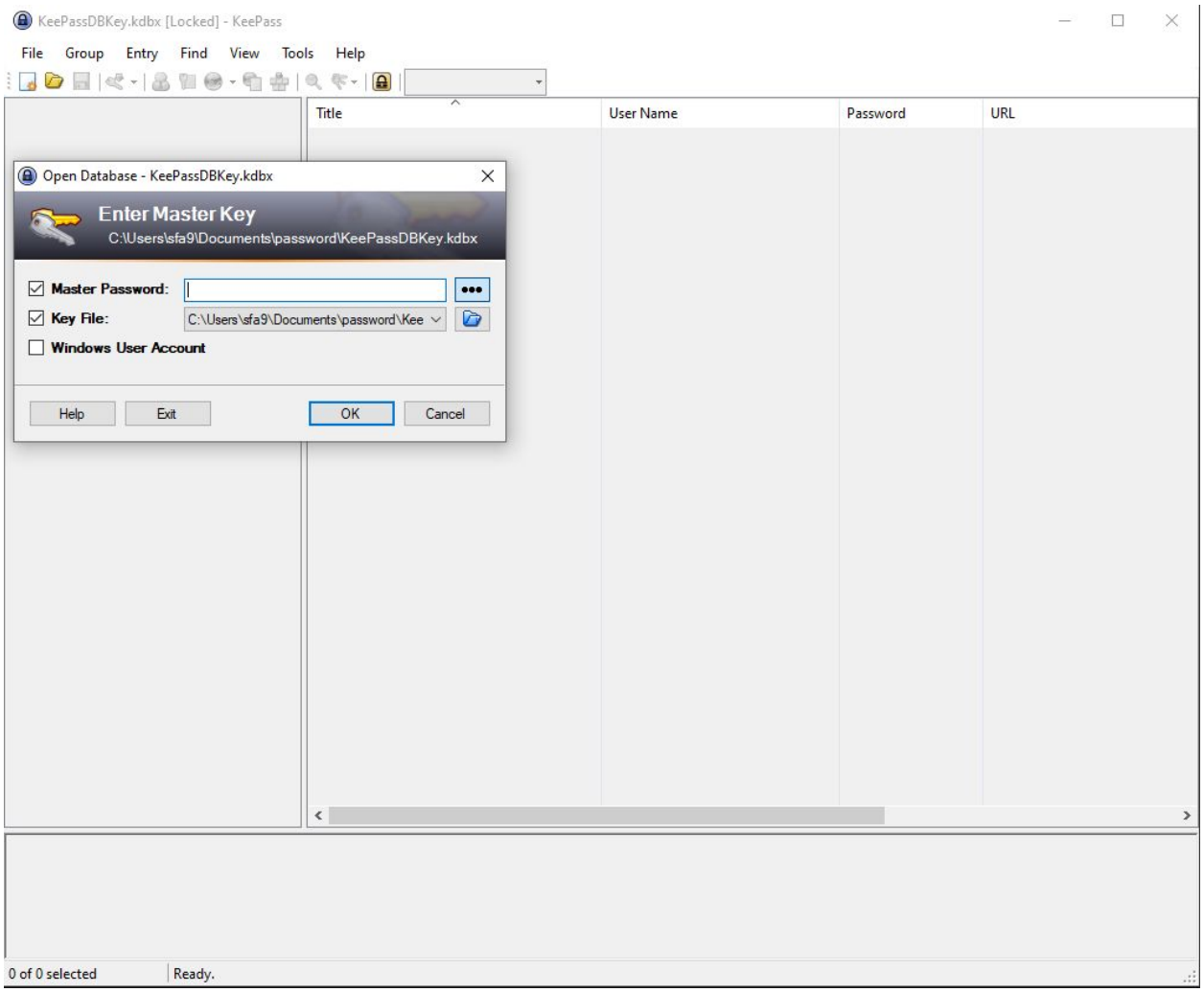
Windows 10.x Approved encryption is BitLocker 128 bit.	
MacOS 11.x	

Ubuntu 20.x	

Set up a password manager

This is only relevant for the A9L SysAdmin Security Group.

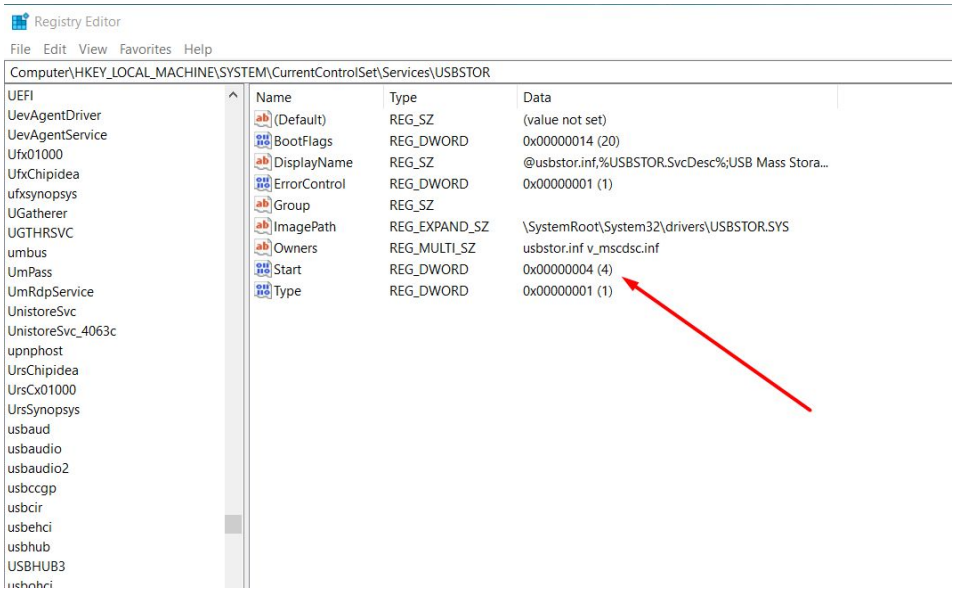
All members of this group are required to use KeePass. It is cross platform and valid for all OS.



Disabling External Media as well as autoplay and autorun

As an extra precaution against insertion of external media, workstations must have autoplay and autorun turned off

OS	Screenshot

Windows 10.x	
MacOS 11.x	Not yet officially implemented. Expected in place February 2021
Ubuntu 20.x	

Allowed Web Browsers and Email clients

Cross platform: