Mobile Device Management from Jamf is safe to use

-This DPIA covers Jamf School, a Mobile Device Management system.

Implementation of the DPIA.

SIVON conducted this DPIA over approximately a two-year period. Jamf has been transparent in the interviews and provided clear insights into the system. Furthermore, Jamf has been receptive to SIVON's suggestions to modify the SLASA, among other things.

-Conclusion

Jamf School is a widely used cloud application used by schools to manage Apple devices from a central environment. From this environment, comprehensive management capabilities can be configured for devices such as Macbooks, iPads, smartphones, their users and classes, as well as for desired apps. The DPIA showed that in terms of information security there are no major risks associated with the use of Jamf school, and there are only a few risks for which schools need to implement their own measures. These will need to be included in the “local DPIA,” and concern the following:

3. Unauthorized access to the admin account, which could compromise the management of Apple devices.

4. The necessity to configure admin roles internally within the organization.

6. The risk of excessively broad administrator rights being granted to users.

7. Issues related to support tickets handled via the support desk.

8. Potential loss of control over access to the Apple Store.

The following adjustments were implemented by Jamf during the course of this DPIA to mitigate identified risks:

1. Preventing unauthorized users from accepting the Jamf terms and conditions.

2. Improving transparency regarding Jamf’s own processing purposes.

5. Adjustments to the data processing agreement to mitigate risks

All the risks and possible measures and measures taken can be found in the following table:

Risk no.	Description of risk (keyword)	Risk	Measure(s) (Org/Techn/Legal)	Measure for (application/school name)	Residual risk (figure)	Explanation of acceptability of residual risk	(date) measure implemented?
1	Agree with Jamf terms by unauthorised user	6	Jamf is creating a revised version of the SLASA and DPA specifically aimed at Dutch schools (a so-called 'special contract'). This agreement will replace the click-through agreement used previously. This new version avoids the click-through and will instead be signed for approval by the schools themselves.	Jamf	0	There is no residual risk after implementing the measures	Agreement made 17 July, 4 December confirmation of implementation
2	Lack of transparency regarding own processing purposes Jamf	6	Jamf will remove Article 19 section c in the same revised version of the SLASA. As a result, Jamf will no longer assume the role of controller. Jamf has confirmed to carry out processing only in the context of product improvement. As Jamf is only a processor of the schools, it is no longer necessary to explain the purposes of its own processing activities.	Jamf	0	There is no residual risk after implementing the measures.	4 December confirmation
3	Unauthorised access to admin account, shut down education with Apple Devices.	3	Limit the number of roles with the highest authority within Jamf to reduce the risk of unauthorised access and unintended changes. This can be done using a strict role-based authorisation matrix.	School	0	There is no residual risk after implementing the measures.	To be set up directly by school management

4	Admin roles must be set up by themselves	6	Proceed carefully when defining admin roles and align them with the authorisations required by the employees/users. Regularly review and update these roles with some regularity.	School	0	There is no residual risk after implementing the measures.	To be set up directly by school management
5a	Data Processing agreement, rights of data subjects	3	Jamf indicates that this restriction only applies to situations where they act as a data controller. Since the contract has been amended in such a way that Jamf is effectively no longer a data controller under contracts with Dutch schools, this measure is no longer necessary and the issue has been resolved.	Jamf	0	There is no residual risk after implementing the measures.	4 December confirmation
5b	Data processing agreement, personal data breach procedure.	6	Jamf summarises its personal data breach procedure so that it can be added to this DPIA. (see pages 55-56)	Jamf	0	There is no residual risk after implementing the measures.	17 July delivered
5c	Data processing agreement, jurisdiction	6	Jamf declares, for the purpose of clarity and providing a trusted legal environment for resolving disputes, that the jurisdiction of the controller applies in the revised version of the SLASA and DPA. This adjustment will be made in Article 14 of the SLASA. Disputes will be settled under	Jamf	0	There is no residual risk after implementing the measures.	Confirmation 4 December

			the laws and dispute resolution procedures of the Netherlands, under Dutch law.				
5d	Data processing agreement, lack of transparency	4	Jamf sends existing customers notifications in case of updates within the list of sub-processors. This is done via email as well as via the 'Jamf Nation', Jamf's user group portal. Schools are advised to keep careful track of these notifications to stay up to date with changes.	Jamf/school	0	There is no residual risk after implementing the measures.	Existing alternative measure
5e/f	Data processing agreement, ambiguity regarding purchased product and personal data to be processed	6	Jamf will provide clarity in the DPA with regard to both the purchased products to which the processing relates as well as to the personal data used in the process, including location data, diagnostic data and photographs. Jamf will add this in the next version of the DPA.	Jamf	0	There is no residual risk after implementing the measures.	Will be implemented in Q1 2025
6	Overly broad administrator rights	4	Implement a structured roles and authorisation policy within the Jamf-School management system. By defining these roles with clearly described permissions that align with users' responsibilities, the risk of unqualified users making unintended changes to settings and functionalities is reduced.	School	1	After implementation, the risk is reduced, but it cannot be completely eliminated.	To be set up directly by school management
7	Support Jamf	4	Make sure to exercise caution and restraint when sharing (sensitive)	School	1	After implementation,	To be applied directly by

			information, such as print screens and documents, for technical support from Jamf's support environment. Share only the information strictly necessary to resolve the support issue. Keep in mind that Jamf processes this support data as a data controller.			the risk is reduced but cannot be completely eliminated	school management
8	Configuration Jamf/access to Apple store	4	Restrict access to the Apple Store for users of Apple devices issued under management, in order to maintain control over the school's digital (learning) environment. This also prevents the school from being able to see what apps the student/employee has downloaded on their device.	School	0	There is no residual risk after implementing the measures.	To be set up directly by school management

For further information please check the Dutch version of the DPIA as published by SIVON.

Disclaimer: This translation was partially made using translation software. No rights can be derived from this translation.