Release of Wiscard Photos to Applications Procedures

Procedures Summary

The Release of Wiscard Photos to Applications Procedures outline the methods by a service would request access to and user what conditions would release be granted to those services.

Who These Procedures Applies To

The Administrative Data Access Provisioning Procedures applies to the Stewards of our Wiscard Photos and to the users of that data.

Procedures

1. Access to Wiscard photo is limited to applications with a business need to perform verification of identity. Applications seeking Wiscard photo must complete an Identity Data Integration request[1] and describe the business process that requires photo verification.
2. Standing Approval – consumption via Photo Web Service. If a request meets the following three conditions, the request will be approved.
    a. Condition #1 – Application must consume photo information from the Photo Web Service[2]
    b. Condition #2 – Application must not store photos locally
    c. Condition #3 – Application does not require photo information for students electing FERPA privacy.
3. Standing – Approval – secure local storage of photo information. If a request does not meet the requirements for #2 above, it then must meet the following five requirements in order for the request to be automatically granted.
    a. Condition #1 – Application will receive an extract of photo information via a secure channel.
    b. Condition #2 – Photos will be watermarked with an appropriate copyright and application-specific tag.
    c. Condition #3 – local storage of photos will comply with the Required Wiscard (Identity) Photograph safeguards. (See appendix A) Photos will not be stored in the cloud.
    d. Condition #4 – Middleware has consulted with Cybersecurity to ensure that storage of Wiscard Photos in consistent with Cybersecurity policy and the Risk Management Framework.[3]
    e. Condition #5 -- Application does not require photo information for students electing FERPA privacy.

[1] HTTPS://IT.WISC.EDU/SERVICES/IAM/
[2]. https://photo.services.wisc.edu/docs/
[3]. https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/

Definitions

Administrative Data: As defined at Data at UW-Madison:

> *"Data that is generated as a result of utilizing enterprise transactional systems, such as student records, employee data, or financial information."*
>
> See https://data.wisc.edu/data-governance/#classifications for a summary of how data is classified into our risk classifications.

[1] HTTPS://IT.WISC.EDU/SERVICES/IAM/
[2]. https://photo.services.wisc.edu/docs/
[3]. https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/

APPENDIX A

Required Wiscard (Identity) Photograph Safeguards

Wiscard photographs are considered sensitive data. The Photo Group sub-committee of IMLG has recommended that suitable administrative, technical and physical safeguards be in place to protect the Wiscard photos.

Application owners should review and comply with University policies and processes related to handling of sensitive information. The requirements and controls can change over time; it the responsibility of 5 data sponsors and recipients to periodically review the information and take the necessary steps to implement up-to-date standards. Storage of Wiscard photos must comply with campus Storage and Encryption Policy. A summary of 6 safeguards for securing Wiscard photos include but are not limited to (please refer to the web site for an up-to-date list):

1. Hardcopy and retention of Wiscard photographs Printed copies of Wiscard photos (e.g. class rosters) should be kept private and not shared. Printed copies of Wiscard photos must have a UW watermark across the images. The printed copy should be shredded when it is no longer needed.

2. Access to Wiscard photographs Access to Wiscard photos is granted for UW-Madison faculty and staff who have a legitimate educational need-to-know. Electronic access to employee and/or student photos must be authenticated and logged by the system that is storing the photos. Access to photos does not imply permission for authorized users to modify, store or share the photos with other persons who do not have a legitimate need-to-know.

3. Storage and retention of Wiscard photographs Storage of Wiscard photographs outside the central photo source system (UDS) should only be done when other acceptable options are not available, and with custodian approval. Administrative policies must be at least as stringent as this policy. Each site storing photos must have a photo retention policy. If photos are removed from the source system, they must be removed from all systems that are storing them.

4. Audit of systems that store photographs. A periodic third-party verification and audit of any system that stores Wiscard photos is required. It is the responsibility of the unit storing the photos to schedule the audit and report its findings to the appropriate data custodian (i.e., Human Resources for employee Wiscard photos and Office of the Registrar for student Wiscard photos) and to OCIS. OCIS is available upon request to conduct these audits

[1] HTTPS://IT.WISC.EDU/SERVICES/IAM/
[2]. https://photo.services.wisc.edu/docs/
[3]. https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/