

DIVISION	REFERENCE NO.
X. Information Technology	10.3
CATEGORY	DATE
10.3 Identity Theft Risk Reduction Policy	Adopted 12/09

1.0 OVERVIEW

The risk to Joliet Junior College ("College") and its students, faculty, and staff from data loss and identity theft is of significant concern. All members of the College community and third party affiliates share in the responsibility of reducing this risk and protecting information for which they have access or custodianship.

2.0 DEFINITIONS

Identity Theft - A fraud committed or attempted using the identifying information of another person without authority.

Red Flag - A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Covered Account - includes all student, employee, or loans that are administered by the College.

Identifying information - Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or student identification number.

3.0 POLICY

The College adopts this policy to help protect students, faculty, staff, and the College from damages related to the loss or misuse of protected and sensitive identifying information.

This policy helps the College:

- Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
- Detect risks when they occur in covered accounts;
- Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
- Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

DIVISION	REFERENCE NO.
X. Information Technology	10.3
CATEGORY	DATE
10.3 Identity Theft Risk Reduction Policy	Adopted 12/09

3.1 **Summary of Responsibilities**

All College departments are responsible for developing departmental operational procedures in support of this policy. Red flag Guidelines will be given to each department for detecting, preventing, and mitigating identity theft. Each department will designate a Red Flag leader responsible for developing their departmental Red Flag procedures and will implement and enforce these procedures, as well as, training their department staff and design more specific or new procedures as needed. These procedures will apply to all personnel that access sensitive identifying information and/or which open new or access existing covered accounts. This includes all parties that may come into contact with covered accounts, such as, contractors, consultants, temporaries, and personnel of third party affiliates.

3.2 **Detection, Prevention, and Mitigation of Identity Theft**

Departments shall review the guidance and apply procedures to assist in detecting “Red Flags.” In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the steps outlined in the guidance, depending on the degree of risk posed by the Red Flag.

Each department should update their departmental procedures relevant to their operations, to reflect changes in risk, based on the published guidance.

3.3 **Response to Identity Theft**

Once potentially fraudulent activity is detected, the College must act quickly, as a rapid appropriate response can protect students, employees, and the College from damages and loss. The Identity Theft Risk Reduction Guidelines will help the department with appropriate responses relevant to Red Flags.

4.0 **PROGRAM ADMINISTRATION**

4.1 **Oversight of the Program**

The College Vice President of Learner Support and Technology Services and the Vice President of Administrative Services will provide oversight for this program. They will designate an individual (or individuals) with the responsibility for leading, developing, implementing and updating this program. This individual(s) will be responsible for ensuring appropriate training of the departmental Red Flag Leaders on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

4.2 **Program Updates**

DIVISION	REFERENCE NO.
X. Information Technology	10.3
CATEGORY	DATE
10.3 Identity Theft Risk Reduction Policy	Adopted 12/09

The program will be periodically reviewed and updated yearly to reflect changes in risks to students, employees, and the soundness of the College from Identity Theft. The review will take into consideration the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities.

4.3 Staff Training and Reporting

College staff responsible for implementing the Program and a designated lead from each respective department shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Department staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify their supervisor and their designated Red Flag leader once they become aware of an incident of Identity Theft or of the College's failure to comply with this Program. On an annual basis College staff responsible for development, implementation, and administration of the Program shall report to the Vice Presidents on compliance with this Program. The report should address such issues as effectiveness of the policy, procedures, and guidelines in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

4.4 Oversight of Service Provider Arrangements

The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.