

PROCEDURE ON THE USE, DISCLOSURE, AND DISPOSAL
OF EMPLOYEE SOCIAL SECURITY NUMBERS

No employee is permitted to access or use social security numbers (SSNs) without express permission of the College.

In addition to the College's normal security and confidentiality policies and practices, only employees authorized as part of their job duties may access records and documents containing employee SSNs. All other employees are prohibited from accessing, viewing or using other employees' SSNs. Prohibited use according to Michigan P.A. 454 of 2004 is:

- Publicly display all or more than 4 sequential digits of the SSN.
- Use all or more than 4 sequential digits of the SSN as the primary account number for an individual.
- Visibly print all or more than 4 sequential digits of the SSN on any identification badge or card, membership card, permit or license.
- Require an individual to use or transmit all or more than 4 sequential digits of his/her SSN over the internet, computer system, or network unless the connection is secure or the transmission is encrypted.
- Require an individual to use or transmit all or more than 4 sequential digits of his/her SSN to gain access to an internet website, computer system or network unless the connection is secure, the transmission is encrypted, or a password or other unique personal identification number or authentication device is also required to gain access to the internet website, computer system, or network.
- Include all or more than 4 sequential digits of the SSN in or on any document or information mailed or otherwise sent to an employee if it is visible on or without manipulation from outside of the envelope or packaging.
- Include all or more than 4 sequential digits of the SSN in any document or information mailed to an employee unless any of the exceptions in the Public Act apply.
- Any exceptions to the above may be found by specifically checking in P.A. 454, and any questions may be directed to the College's Director of Human Resources.

All documents and records containing SSNs and identification information will be kept in a secure environment with need-to-know access by authorized personnel only. When necessary, documents containing this and other confidential information will be properly destroyed through shredding or other means before disposal.

Any employee or individual that accesses social security data without authorization or for illegal purposes shall be disciplined up to and including termination. If illegal intent is determined, employees will be referred to authorities for possible criminal prosecution.