Policy title	Category
Wire Fraud Reduction Policy	Business Office Human Resources
Owner	**Approved by**
Business Office	Ad Council

Purpose of this policy

The purpose of this policy is to establish procedures related to wire transfers from Nebraska Wesleyan University bank accounts. These procedures are designed to reduce or eliminate the risk of wire transfer fraud and the losses suffered as a result of being a wire transfer fraud victim.

Application of this policy

This policy applies to all Nebraska Wesleyan University employees. The primary persons who will be impacted are those persons with access to financial systems, but all employees are required to follow the protocols contained in this document.

Policy statement

Wire-transfer fraud is when Nebraska Wesleyan University employees are deceived by criminals to wire money to a bank account controlled by the criminals.

This policy requires that procedures be established for outgoing wire payments to reduce the likelihood that wire transfer fraud is perpetuated on Nebraska Wesleyan University employees.

These procedures must include the following.

- Establish specific wire instructions with any new business partner who may receive wire payments from Nebraska Wesleyan University. These instructions must include the contact information of a designated individual or department at the business partner that can be reached to confirm a wire or a wire transfer change request. At the same time, Nebraska Wesleyan University shall provide the business partner with similar contact information.
- Independently verify over the phone all wire transfer requests and changes to wire instructions using a known and trusted phone number — not one from the current wire transfer request. The contact information provided in the request must not be used to verify the request.
- Consummate all wire transfers and any new instructions or changes to existing wire instructions with dual control (e.g. two employees).
- Designate employees who are authorized to send wire transfers. All other employees are prohibited from wiring payments.
- Treat all changes to wire instructions and urgent requests to wire funds with skepticism and presume them fraudulent until verified for authenticity.
- Establish procedures for reporting suspected fraudulent wire transfer requests so that other employees may be alerted to the scam.

- Verify with bank to confirm both the account number and the name on the intended/requested account before sending a wire.
- Establish internal procedures for any internal requests to wire funds or change wire instructions and train employees accordingly.

WIRE FRAUD TRAINING AND AWARENESS PROGRAM

This policy requires that an employee wire fraud education and awareness training program be established. This training shall include periodic training so that employees can understand and detect wire transfer scams.

The training shall include instructions on:

- How to closely inspect all emails related to wire transfers for signs of fraud;
- The relevant procedures created as a result of this policy;
- How to report suspected wire fraud requests;
- How and when (immediately) to report any fraudulent payments; and
- Any other items that Nebraska Wesleyan University IT security team determines will help reduce the risk of being victimized by wire fraud.

The program shall also include periodic reminders to employees of the ongoing risk of wire fraud and ensure employees are following proper procedures.

REPORTING PROCEDURES

This policy requires that procedures be established and followed if Nebraska Wesleyan University has been the victim of wire fraud.

These procedures may include:

- Notify the receiving bank and request that a freeze be placed on any remaining funds.
- Immediately notify Nebraska Wesleyan University's Crime Policy insurance carrier. Note: this is EIIA.
    - If an Institution does not immediately report this issue to EIIA, there can be a problem with coverage.
- Notify law enforcement after seeking advice of counsel.
- Investigate whether the email system may have been compromised.
- Ask business partners to investigate whether their email systems may have been compromised.

POLICY COMPLIANCE

Compliance Measurement

Compliance with this policy will be verified through various methods, including but not limited to, internal reviews, and continued feedback of the Controller.

Exceptions

Any exception to the policy must be approved by the Vice President for Finance and Administration in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.