|  |
| --- |
| **BRT Group POLICY & PROCEDURES** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Title:** | **Wire Transfers** | **Policy Number:** |  |
| **Effective Date:** | **December 4 2019** | **Revision Number:**  **Replaces:** |  |
| **Prepared By:** | **Amanda Stolzer** | **Approved By:** |  |

Effective immediately!

If anyone or any company informs us that their bank account information has changed – We must have this confirmed both in writing and **verbally/by text message.** Including employees of BRT. Hackers can use owners names and email addresses to make it look like the request came from them (example: Phil Burrett [phil@brtgroup.com](mailto:phil@brtgroup.com))

We cannot just accept emails stating that a supplier/ customers bank account has changed.

Hackers can hack into someone’s email address and request a change to their bank account, be aware as it can look the same as a legitimate email. This is why we must also follow up with a phone call (verbal), or a text message (different phone number that a hacker won’t know) to ensure that person did request the bank account change.

Always have someone else check changes or modifications to bank accounts on wire transfer templates.

Do not rush to pay wire transfers – Always double check that the information is correct.

Once a wire transfer has been sent – we cannot stop or retrieve it. The money is then gone from our account.

Hackers have also disguised themselves as OPP/RCMP Police/CRA/IRS – never give out personal information or send money to anyone unless authorized by a manager and they made sure it was legitimate.

Never give out Social Insurance Numbers, Social Security Numbers (USA), Bank account numbers etc..

NEVER give out the key fob number to anyone! The real bank would never ask for this information over the phone or by email.