November 8, 2023

The Andersons, Inc. Cybersecurity Program Statement

The Andersons is committed to ensuring the safe operation of its business by means of a dedicated Information Security program designed to protect the confidentiality, integrity, and availability of its assets. These protections extend to the data that is exchanged with customers which is stored and processed by The Andersons.

To achieve these objectives, The Andersons has implemented multiple industry-recognized cybersecurity best practices, outlined at a high-level below:

Identify: Proactive Risk Management

1. The Andersons Information Security program aligns closely with NIST CSF 1.1, which has been the target framework for multiple years.
2. The Andersons maintains an inventory of physical and digital assets in-use throughout the environment.
3. The Andersons has an established vulnerability management program, which regularly scans this inventory for known risks and prioritizes remediation efforts accordingly.

Protect: Damage Prevention

1. The Andersons automatically measures user behavior for anomalous and risky activity and has automation in place to revoke access should such an incident be identified.
2. The Andersons limits a user's ability to access company resources unless they pass a series of strict requirements. This includes, but is not limited to, conditional access restrictions, Multi-factor Authentication (MFA), and Role-based Access Control (RBAC) restrictions and requirements.
3. The Andersons performs regular cybersecurity awareness training. As part of this effort, users are regularly sent targeted phishing simulations to maintain a high level of awareness of such risks, and to identify targeted training opportunities.
4. By default, The Andersons encrypts data-at-rest on company computers.

5. By default, The Andersons installs antimalware and Endpoint Detection and Response (EDR) technologies on company computers.
6. Specific sensitive and regulated data types are automatically identified and protected as necessary.
7. The Andersons has established a regular maintenance period schedule for assets to accommodate for impactful patching and update efforts.

Detect: Recognize Actualized Risks

1. The Andersons has multiple mechanisms in place to detect and respond to anomalies across the environment. Anomalies are automatically prioritized and appropriately investigated by a team of trained analysts.
2. The Andersons continuously monitors cybersecurity intelligence feeds to understand and detect new and emerging cyber threats.
3. The Andersons has centralized immutable logging in place with long retention policies to accommodate incident response, threat hunting, and root-cause analysis efforts.
4. The Andersons has 24/7/365 Security Operations Center (SOC) coverage which escalates anomalies for analyst review.

Respond: React to Identified Risks

1. The Andersons has a dedicated Cybersecurity Incident Response policy, plan, and procedures in place to appropriately respond to detected threats.
2. The Andersons performs root-cause analysis on incidents of sufficient risk or impact.
3. The Andersons regularly exercises the plan to test familiarity and to identify gaps.
4. The Andersons regularly conducts 3rd party penetration tests to identify control and training gaps.
5. The Andersons information security team receives dedicated incident response training, certifications, and other resources to ensure efficient response efforts.
6. The Andersons has established procedures for involving law enforcement and any other relevant external stakeholders.
7. The Andersons maintains a dedicated 3rd party incident response and digital forensics retainer.

Recover: Reduce Impact

1. The Andersons performs regular backups which remain immutable for the entire retention period.
2. The Andersons performs regular disaster recovery exercises.
3. The Andersons maintains a physically separate alternate data processing site.
4. The Andersons maintains and regularly exercises a crisis communications plan.

If you have any questions or concerns, feel free to reach out at info-sec@andersonsinc.com for more information.

LEGAL DISCLAIMER: THIS DOCUMENT WAS DESIGNED STRICTLY FOR THE PURPOSE OF PROVIDING GENERAL HIGH-LEVEL INFORMATION REGARDING THE CURRENT STATE OF THE ANDERSONS' CYBERSECURITY PROGRAM AND REPRESENTS A "SNAPSHOT-IN-TIME" OF THE STATE OF THE CYBERSECURITY PROGRAM AS OF THE DATE OF THIS STATEMENT. THIS DOCUMENT IS NOT INTENDED TO CREATE A CONTRACTUAL RELATIONSHIP BETWEEN THE ANDERSONS AND ANY OTHER PARTY, AND DOES NOT CONSTITUTE AN OFFER TO ENTER INTO, NOR SHALL IT BE CONSTRUED AS, NOW OR IN THE FUTURE, A CONTRACT OR PROMISE BY THE ANDERSONS TO PERFORM ANY SPECIFIC TASKS OR TO ASSUME ANY LIABILITY RELATED TO CYBERSECURITY ON BEHALF OF ANY PARTY, AND SPECIFICALLY DISCLAIMS ANY SUCH LIABILITY. NOTHING IN THIS DOCUMENT SHALL BE CONSTRUED AS A GUARANTEE OR WARRANTY OF ANY KIND REGARDING THE ANDERSONS CYBERSECURITY PRACTICES, AND ANY AND ALL SUCH GUARANTEES AND/OR WARRANTIES, EXPRESS OR IMPLIED, ARE HEREBY DISCLAIMED IN THEIR ENTIRETY. THE NATURE OF CYBERSECURITY THREATS IS FAST-MOVING, AND RESPONDING TO SUCH THREATS REQUIRES CONSTANT RE-EVALUATION AND SOMETIMES MODIFICATION OF OUR CYBERSECURITY PROGRAM. THE ANDERSONS THEREFORE RESERVES THE RIGHT, AT ANY TIME AND WITHOUT NOTICE, TO CHANGE, MODIFY, DELETE, OR ADD INDIVIDUAL ELEMENTS OF ITS CYBERSECURITY PROGRAM, INCLUDING THOSE NOTED ABOVE.