MSCI/BCTIM CYBER INFORMATION TECHNOLOGY SECURITY CHECKLIST

Self Rank			Security Policy Governance
Y	N	In Progress	Information security responsibilities have been assigned and are understood throughout the organization
Y	N	In Progress	Purpose, scope, roles, responsibilities, and implementation programs surrounding IT security are well defined
Y	N	In Progress	Confidentiality or non-disclosure agreements are implemented with any third party, external entities
Y	N	In Progress	Third party assessment tools are used to test suitability and effectiveness of implemented security measures regularly
Y	N	In Progress	A formal overview document detailing the security requirements for IT systems and its enforcement exists
Y	N	In Progress	All changes to IT systems are documented
Y	N	In Progress	IT system changes are reviewed against established security protocols
Y	N	In Progress	Systems and information are classified by value to critical business functions
Y	N	In Progress	Systems and information are classified by level of security required
Y	N	In Progress	IT training is provided to all employees and contractors
Y	N	In Progress	IT training includes terms on acceptable use, good computing practices, legal policy and consequences
Y	N	In Progress	Access levels are based on job function
Y	N	In Progress	New hires who will gain access are screened for security prior to hire
Y	N	In Progress	Company has policies to ensure the return of company related property and information when employees are terminated
Y	N	In Progress	Company has policies and procedures to identify and report when a security flaw is detected
Y	N	In Progress	Company is equipped with policies and procedures that security flaws can be corrected in a timely manner
Y	N	In Progress	Company uses most up to date WiFi protocols and enables new security measures as it becomes available

Self Rank			Information and Data Security
Y	N	In Progress	Company uses an automated IT monitoring system that audits system logging, security events, system use, and failures
Y	N	In Progress	Data is classified in terms of its sensitivity and criticality to critical business functions
Y	N	In Progress	Company has policies and procedures to ensure individuals have the correct level of access
Y	N	In Progress	Company mandates that users have non-simple passwords
Y	N	In Progress	Periodic password changes are required
Y	N	In Progress	Data is protected from unauthorized disclosure during transmission
Y	N	In Progress	Wireless internet access is restricted to company issued devices only, or, non-company devices only have limited access to wireless network
Y	N	In Progress	External Access to company systems is only allowed through a secure access portal, e.g. VPN
Y	N	In Progress	Employees only receive the lowest privilege level necessary to execute the business functions for which they are responsible
Y	N	In Progress	Physical media is labeled with security and handling requirements
Y	N	In Progress	Company has appropriate destruction and disposal methods for physical and virtual media
Y	N	In Progress	Physical media is password protected and encrypted
Y	N	In Progress	Company has policies and procedures in place to recover critical and sensitive information
Y	N	In Progress	System and data backups are created on a regular basis
Y	N	In Progress	System and data backups are stored in multiple offsite locations
Y	N	In Progress	Safe email practices including; employee training regarding safe email practices, automatic virus and malware scanning, and attachment security protocols
Y	N	In Progress	Two factor authentication for email, calendar, computer login, etc.
Y	N	In Progress	External cloud storage is blocked (e.g. Personal Google Drive/Dropbox)
Y	N	In Progress	Company used external cloud storage is encrypted and secure

Self Rank			Employee Device Checklist
Y	N	In Progress	Device OS and applications are updated to the most recent versions
Y	N	In Progress	Devices feature automatic, timed locking after periods of inactivity
Y	N	In Progress	Devices are encrypted and password protected
Y	N	In Progress	Devices are VPN enabled
Y	N	In Progress	Developer Debug access is disabled
Y	N	In Progress	Device administrator level access is restricted to IT department
Y	N	In Progress	Work emails and calendar access is only available on company devices
Y	N	In Progress	Remote-wipe is enabled on all devices
Y	N	In Progress	Data is stored on company servers rather than locally
Y	N	In Progress	Data is not stored on personal USB drivers
Y	N	In Progress	All work email is sent through company email and NOT personal email
Y	N	In Progress	BYOD is restricted and not available for most employees
Y	N	In Progress	Company limits access to personal cloud storage
Y	N	In Progress	Access to apps and websites on work devices is monitored and limited to those that are work necessary
Y	N	In Progress	Company uses high level ISP blocking, restricting access to websites, e.g. blocking of all personals and data websites, adult content websites, etc.
Y	N	In Progress	Company restricts in office social media activities and establish social media protocol for employees
Y	N	In Progress	Social media posting related to work is strictly prohibited or monitored

Washington University in St. Louis OLIN BUSINESS SCHOOL | BCTIM

Metals Service Center Institute 100 YEARS STRONG™

Metals Service Center Institute | 4201 Euclid Ave Rolling Meadows, IL 60008 | Phone: 847-485-3000 | Fax: 847-485-3001