X-RITE Security Technical and Organizational Measures
(last updated March 2023)

X-Rite IT Security Definition

IT security at X-Rite means guaranteeing the confidentiality, integrity, availability, and compliance of all corporate information stored, processed, transported and represented by IT systems under the control and responsibility of X-Rite in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities.

X-Rite IT Security Technical & Organizational Measures (in general)

1 IT Security Program

1.1 Program Governance & Responsibilities

- The X-Rite IT Security Program is led by the Platform Chief Information Security Officer (Platform CISO). IT Security is responsible for the vision, mission, objectives, and services delivered to X-Rite departments to enable appropriate and reasonable protection of information and information assets across the organization.
- IT Security is a shared responsibility. The Platform CISO will work with all departments to ensure effective and timely implementation of the X-Rite IT Security Policy through alignment with business priorities and following a risk-based approach.
- The Platform CISO is responsible for ensuring that the actions and controls within this policy are carried out within their organizations. The Platform CISO is also responsible for ensuring that all users are aware of policies related to IT Security.
- In case personal data is involved, the Data Protection Officer (DPO) is involved.

1.2 IT Security Coordination

IT Security coordination is performed by the Platform CISO and implemented by departments. The IT Security Program will be maintained and monitored through the following:

- Developing, reviewing and approving the IT Security Policy (including any companion and/or supplemental policy documents) and overall responsibilities;
- Performing IT security risk assessments and accompanying risk reduction and management strategies;
- Maintaining IT security strategy;
- Ensuring that IT Security is part of the X-Rite planning process;
- Reviewing and approving exceptions to IT Security policies and standards;
- Ensuring adherence to IT Security policies and standards;
- Ensuring adherence to legal and regulatory compliance requirements pertaining to IT Security;
- Reviewing IT security incidents as necessary; and
- Monitoring changes in the exposure of information and IT assets to IT security threats.

2 Acceptable Use Policy

The Acceptable Use Policy (AUP) defines appropriate uses of data and IT assets by users. Users shall keep confidential the use of all internal IT Security mechanisms and controls unless otherwise authorized to disclose certain information.

Confidential - Company Proprietary

2.1 Acceptable Use

- Users shall maintain all proprietary data stored on any information storage or processing devices or systems in accordance with this policy.
- Immediately report any actual or possible theft or unauthorized use of your password, data, or assigned IT assets to the IT department in accordance with local procedures.
- Users must exercise caution when interacting with email message attachments and website links as they may contain phishing or malicious software.
- Users may access, use, or share data only to the extent it is required and users are authorized to do so to fulfil their assigned job duties, or as permitted by applicable local law.
- Users must take reasonable precautions to ensure their password is protected against loss, theft, compromise, or misuse by an individual.
- Users may use software purchased by X-Rite only for its intended business purpose consistent with IT department policies for software installation.
- All X-Rite computers and mobile devices must be password protected with an active automatic screen lock feature. Users must lock their device when it is unattended and never leave a device unattended in a public place.
- Users are responsible for protecting against the loss, theft, or damage to all IT assets assigned to users including but not limited to computer systems, mobile devices and portable storage drives Users have been issued.
- Measures are taken to prevent the spread of viruses, worms, phishing email messages, and malicious software by not installing unauthorized software, being careful when clicking on any links contained in e-mails, and not opening links or attachments from unexpected senders.
- Users may only use IT assets to make statements on social media and other external media in accordance with the Code of Conduct.
- Incidental personal use of IT assets is permitted. Users are responsible for exercising good judgement regarding the reasonableness of personal use of IT assets. X-Rite is responsible for creating guidelines concerning personal use of computer systems for personal use, including internet usage, consistent with any applicable collective bargaining agreement and where applicable, local laws, regulations & Workers Councils.

2.2 Inappropriate Use

- Using IT assets in a manner that jeopardizes the confidentiality, integrity, or availability or safety of the information resources.
- Using IT assets in violation of applicable laws or regulations.
- Using IT assets to access, display, send, receive, store, create, or transmit images or communications that mock, degrade, or a disrespectful of a protected class or an individual's legally protected characteristics.
- Using IT assets to access, display, send, receive, store, create, or transmit pornography or sexually explicit images or communications.

2.2.1 Inappropriate Uses of Email, Instant Messaging and Communications

- Includes, but is not limited to, the following:
    - Using email or instant messaging for more than incidental personal reasons;
    - Sending or forwarding business (i.e., non-personal) email from an email account to a personal or non-
      X-Rite account without prior authorization by IT and/or IT Security;
    - Any form of personal harassment;
    - Forwarding electronic chain letters;
    - Using an email or instant messaging account for unauthorized solicitation purposes or promotions;

- Using an email or instant messaging account for purposes outside of your assigned job duties or excessive personal use; and
- Using an email account to state or imply that you are authorized to speak on behalf of X-Rite unless explicitly authorized to do so

2.2.2 Inappropriate Uses of IT assets.

- Includes, but is not limited to, the following:
  - Using another individual's account or attempting to capture or guess other users' passwords;
  - Sharing passwords with others or allowing someone other than yourself to use your password;
  - Allowing unauthorized users to access the network by using an IT asset that is connected to the X-Rite system;
  - Tampering with, disabling, or otherwise interfering with security controls on an IT asset or the X-Rite network;
  - Installing software for personal use on an IT asset unless authorized by the IT department;
  - Unauthorized access, transmission, or distribution of copyrighted materials where users do not have an active license;
  - Violating of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of “pirated” software/content products that are not appropriately licensed for use by X-Rite as applicable;
  - Using or installing software applications or technologies that have not been approved by IT department;
  - Attempting to access restricted portions of the X-Rite network, an operating system, security software, or other administrative applications without prior authorization by the system owner or administrator;
  - Using IT assets in conjunction with the execution of programs, software, or processes that are intended to disrupt (or that could reasonably be expected to disrupt) other computers or network users, or damage or degrade performance, software, or hardware components of a system;
  - Using tools that are normally used to assess security or to attack computer systems or networks unless you have been specifically authorized to do so by IT Security;
  - Knowingly establishing, or causing to be established, communications to systems that could allow unauthorized access to IT assets; and
  - Using IT assets other than for their intended and authorized purposes, including but not limited to mining cryptocurrency and operating or assisting in the operation of a non-X-Rite business.

3 Risk Assessment and Management

- IT Security risk assessments are important to maintaining appropriate business risk management practices. IT Security is responsible for identifying, assessing, and articulating security threats and vulnerabilities by performing risk assessment procedures.
- IT risk assessment procedures are to be performed when there is or likely to be changes to operational, financial, reputational, or organizational risk level resulting from the contract, project, or initiative.
- X-Rite acceptance is required commensurate with the identified risk level.

4 Compliance

4.1 Authorized Software

- X-Rite associates may only download or otherwise use appropriately licensed software authorized by the Procurement and IT department on IT assets.
- Software piracy and illegal sharing or re-distribution of licensed software is prohibited.
- Any General Public License (GPL) software must have IT and IT Security reviews performed prior to adoption.

4.2 Personal Device Usage

- On occasion and with X-Rite prior written approval, personal devices may be used to access IT assets or view data.
- X-Rite has a written Personal Device Usage policy that complies with personal data privacy laws prior to allowing users to bring their own device to access IT Assets or view data in the event a personal device is used for more than 60 days in a 180-day period or in-lieu of an X-Rite issued device.
- Users are responsible for maintaining and protecting personal devices which are not owned by X-Rite at all times.
- Personal devices must be kept up-to-date with software and security patches applied at least once per month.
- Personal devices must be configured with a secure password that complies with password requirements. Mobile devices must be configured to automatically erase the contents (wipe) of the device if an invalid password is entered 10 times.
- Personal devices are not allowed to be connected directly to X-Rite networks unless otherwise permitted by the Personal Device Usage policy.
- Personal devices must be immediately removed from X-Rite networks upon notification and direction from IT or IT Security.
- X-Rite data must not be stored on a personal device.

5 Data Privacy

- Each associate and department must adhere to the Global Privacy Policy and the Privacy Compliance Manual.

6 Security Awareness

- IT Security will develop and implement an IT Security awareness program.
- IT Security responsibilities shall be communicated during new-hire orientation sessions by the HR department.
- All associates who use or access information systems must participate in all IT security awareness training and education exercises.
- IT Security will provide regular training reinforcement through techniques such as webinars, posters, current-event cyber security news articles posted on internal portals, lunch and learn sessions, and/or e-mailed security reminders.

7 Security Event Management and Reporting

- A comprehensive IT Security Event Response Management approach shall be established to govern the general response, documentation, and reporting of events affecting IT resources that includes defined roles and responsibilities and covers the monitoring, detection and response to potential security threats and events, as well as reporting suspicious activity and weaknesses.
- All associates should report all known or suspected IT security events in an expeditious and confidential manner to IT and IT Security.
- IT must immediately upon identification escalate the occurrence of a suspected event to IT Security for further analysis and evaluation, as required by the Legal and Compliance Escalation Policy. If evaluation reveals the data contains personal data, then the Data Protection Leader (DPL) must be notified immediately and will determine if the local data protection authority must be contacted.
- In case the security event involves customer data, Platform Security shall report all security events to customers as soon as possible after confirmation. This shall include the following in the email notification:
    - Description of the nature and scope of the suspected security event
    - Potential impact on the delivery of contracted goods or services to the customer
    - Potential impact on personal data including the number of subjects and records impacted
    - Status on steps taken to mitigate the incident and minimize reoccurrence
    - Name and contact details of the Platform CISO and the Platform DPO (data protection officer)
- Only Danaher Information Security may formally declare the occurrence of an IT incident. X-Rite is responsible for maintaining information system logs and audit trails that may be used for forensic investigation purposes. Audit trails must be readable, exportable, and able to be presented to IT Security if requested during an IT incident response.
- X-Rite shall support and fully comply with investigate procedures during an IT security event or with an external forensic incident response organization for such purpose. Upon request, interim reports on the results of any responsive forensic investigation and remediation efforts will be available.

8 Data Management and Protection

8.1 Data Lifecycle Protections

- A comprehensive Data Classification Standard shall be established and adhered to for the appropriate handling, processing and retention of data.
- Data retention periods must be formally documented and approved by X-Rite to ensure they meet business and regulatory requirements; data shall be retained according to the documented schedules.
- Encryption of data shall be implemented based on the classification and sensitivity of the data in question and must use strong encryption algorithms.
- Local standards shall be developed for the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys.
- Documented minimum security baseline standards will be developed for IT assets and data. These configurations must adhere to these documented security standards.
- Procedures for managing and safe disposal of removable media, such as tapes, USB devices, external hard disks, and printed reports shall be developed and implemented.
- Procedures for the secure disposal of data and media shall be established. Unneeded data and media shall be disposed of in accordance with industry-accepted standards for secure deletion and/or destruction. Disposal of data containing personal data must comply with the Privacy Compliance Manual.

8.2 Backups

- X-Rite will establish and adhere to documented data backup standards to ensure the availability of organizational data.

- Back-ups necessary to facilitate operational continuity must be stored in an environmentally protected location that may or may not reside in the same location as production data. Back-ups are not to be written on the same hardware and must be afforded the same level of security and protections as was intended for the original data set.
- Back-ups necessary to facilitate disaster recovery activities must be stored in an environmentally protected and access-controlled site that has a geographically different risk assessment than the source/production data (on premises or in the cloud) and would not be impacted by a natural disaster.
- Backup data must be afforded the same level of security and protections intended for the original data set.

9 Identity and Access Management (IAM)

X-Rite is responsible for the assignment and management of official identities. IAM is critical to ensuring that unauthorized access to information, systems, applications, and physical areas is prevented.

9.1 Account Management

9.1.1 Provisioning

- All system users including vendors and contractors must utilize a unique ID and password to access information systems. Access to any systems or data may only be granted after obtaining appropriate managerial signoff.
- Requests for new access shall be made using defined procedures. Vendor and contractor accounts must be set to expire upon termination of contract or onsite work at the time these accounts are created and shall be monitored while in use.
- Access shall be granted on the principles of need-to-know and least privilege.
- Access can either be provided by individual requests or, preferably, through role-based approval. The role-based access control approval consists of management approval of pre-set access for a given role within the organization. Deviations from the standard pre-approved roles require additional approval from X-Rite leadership.

9.1.2 Deprovisioning

- Notification of terminations must be provided by X-Rite Human Resources to the IT department within five (5) calendar days.
- Notification of involuntary employment separations must be sent to IT administrators for de-provisioning as soon as the termination occurs.
- The X-Rite IT department must de-provision access to IT assets and data within 2 calendar days of notification from Human Resources.

9.1.3 Job Change Transfer

- All job change transfers must be recorded in the HR system of record prior to the change taking place.
- All access to IT assets and data is required to be reviewed against the requirements of the new role for applicability.

9.1.4 Shared and Service Accounts

- The use of shared, common-use identifiers for systems across multiple support staff members is not permitted.
- Where the elimination of shared IDs and passwords is not technically feasible, they must be stored in a secure, encrypted password vault. The password must be changed each time the account is accessed such as to prevent saving of the account password.
- Any dedicated application service account must grant the least level of privilege possible and adhere to strong password strength requirements. Applications must have uniquely setup and maintained service accounts.

- All X-Rite application service accounts must have an assigned owner and validated business justification that is stored in a central repository.
- X-Rite service account passwords will follow password policy requirements; the minimum password length required for administrator passwords is 15 characters.
- The use of X-Rite service accounts is restricted to applications only.
- All X-Rite service accounts must be reviewed at least annually for applicability and ownership.

9.1.5 Dormant Accounts

- All dormant accounts will have access disabled after not incurring a valid authentication for at least 90 days.

9.1.6 Access Reviews

- All active X-Rite administrator accounts for critical systems must be reviewed at least quarterly to ensure all accounts are still necessary, belong to active employees or have a valid functional use, and have appropriate access rights within systems.
- On a quarterly basis, all third-party access must be reviewed to ensure that all contractors and vendors still require system access.
- Management reviews must be performed to identify and address excessive access and potential segregation of duties conflicts across applications.
- Segregation of duties access reviews must be performed by an individual separate from those administering the systems to ensure independence of the review.

9.2 Authentication Practices

Minimum authentication requirements must be met by all IT assets and data. This is applicable for all IT systems that have network connectivity including individual and departmental accounts, applications, systems and device.

9.2.1 Minimum Password/Passphrase Requirements

Passwords/passphrases must be secured and are considered confidential data. All accounts must be set to meet minimum password/passphrase requirements, or password/passphrases of at least equivalent strength, unless functionally restricted. The current release of NIST Special Publication 800-63-3 – Digital Identities Guidelines must be considered for guidance.

- Minimum password requirements are as follows:
    - Minimum password length of 15 characters;
    - Must contain 3 of the following:
        - Upper case alphabetic;
        - Lower case alphabetic;
        - Numeric; and
        - Special character;
    - Maximum password age of 180 days;
    - You may not re-use the previous 10 passwords;
    - Password complexity must be enforced;
    - Over half of new characters in a modified password must be different compared to the previous password to prohibit password incrementing;
    - Forced to change after initial authentication;
    - Incorrect passwords must result in an account being locked out:
        - After no more than 6 incorrect attempts; and
        - Until an administrator unlocks the account (higher security) or a predetermined period of time greater than or equal to 30 minutes (lower security); and
    - Passwords must not be found in the dictionary and must not reflect the user's personal life or account name.

- Users must choose difficult-to-guess passwords and must use different passwords for each application. Using common passwords across multiple platforms could significantly impact the breach of all systems if the password is compromised.
- First time passwords issued by IT must have 15 characters, randomly generated and changed upon first log in.

9.2.2 Password/Passphrase Resets

- IT user identity must be verified before a password may be reset.
- When a password is reset or issued to new users, it shall be a unique value not known by individual's other than the administrator resetting the password and the user, and the password must be changed upon first login.
- Resets will always be communicated via a different communication channel than the channel used for userid.

9.2.3 Authentication Requirements

- Access to critical IT systems shall be authenticated through a centralized identity and authentication repository.
- The use of Multi-Factor Authentication/Adaptive Authentication is required to gain access to designated systems as determined through the IT risk assessment process.
- All authentication is required via the use of encrypted protocols.

9.2.4 Additional Cloud Considerations

- All cloud accounts must be affiliated to an issued account and tied to a system of record.

9.3 Administrator Account Management

9.3.1 Administrator Privileged Access

- Administrative rights and access to an end-user device is a privilege only provided to designated associates with validated business justification for the access.
- All associates with administrator access are required to maintain separate accounts, one with user access and one with administrator access. The usernames and passwords for the two separate accounts are to be unique to each account, and have no replication between them.
- A privileged account management system is implemented for secure storage of administrator user names and passwords.
- Procedures shall be established such that any shared passwords are reset when someone with knowledge of the password separates from the organization.
- Administrator passwords will follow password policy requirements; the minimum password length required for administrator passwords is 15 characters.
- Administrator access to systems hosted in public clouds must require Multi-Factor Authentication, identity protection, and user account compromise notifications.

9.3.2 Segregation of Duties

- All requests for new hires and access changes must take consideration of the possible segregation of duties conflicts the access changes will reflect. It is the responsibility of both management and the administrators to ensure proper segregation and prevent excessive access to any systems.
- Appropriate due diligence must be performed to ensure access granted to an individual does not conflict with other business duties.

10 Third Party Management

10.1 Due Diligence and Risk Assessment

- Due-diligence, including but not limited to investigation into company history/performance and risk assessment, must be performed prior to sharing sensitive data with third party service providers.
- X-Rite business sponsors, Procurement and IT/Security teams must formally approve all third-party service provider risk reviews prior to contract signing, while IT Security will approve all enterprise-level security reviews.

10.2 Responsibilities and Contractual Agreements

- Third party service providers must formally accept responsibility for the security of maintained data, continued compliance with regulatory or industry requirements, and adherence to established service level agreements (SLAs) in executed contracts.

10.3 Monitoring Program

- Procurement and IT Security must track and monitor the compliance of third parties with security requirements on an annual basis.
    - maintaining a complete inventory of third parties who store, transmit, access or process data. This inventory tracks the inherent risk rating for each set of services being provided by the third party and the systems and data to which they have access.
    - monitoring third party compliance with security requirements outlined in the agreement between the third party and X-Rite and shall provide written confirmation of compliance with subcontractor due diligence activities upon request.
    - having a formal third party risk management policy or an equivalent policy/procedure that covers onboarding, monitoring and termination for third party providers.

11 Cloud Security Protections and Considerations

- X-Rite shall establish governance functions to ensure effective and sustainable cloud management processes that result in transparency of information security decisions, responsibility, and operations in alignment with industry standards.
    - The cloud service provider must adhere to all third party due diligence, risk assessment, compliance, contractual, and monitoring requirements.
    - Services obtained by a cloud services provider must follow standard procurement programs. X-Rite associates may not procure cloud services on a credit card and request reimbursement.
    - Roles and responsibilities need to be formally defined in a Service Agreement, Contract, or Master Service Agreement.
    - Network and architectural diagrams are required to be updated with connection details to any cloud service provider.
    - The cloud service provider must have the same level of compliance, regulatory, and/or security requirements as X-Rite would place on the same data.
    - The cloud service provider must have a formalized security program and ideally have a third party accredited firm perform an annual attestation on their internal controls and generate a report to be shared.
- X-Rite secures the systems and data stored, processed, and transmitted through its cloud services and infrastructure.
- X-Rite encrypts all data in the cloud at rest and in transit.
- X-Rite has a formal mechanism in place to access, store or destroy the cryptographic keys used to encrypt data in the cloud.

11.1 Contracts

To ensure the integrity of X-Rite data, all contracts with cloud service providers must address the following, at a minimum:

- Cloud Service Providers are prohibited from mining X-Rite data at any time without explicit written authorization of X-Rite.
- If the Cloud Service Provider will store or have access to Confidential, Restricted or Personal Data, standard privacy language for vendor contracts must be included.
- Cloud Service Providers must fully cooperate with any legal investigations (including e-discovery) in a timely manner, required as a part of a security breach.
- The location of data and any geographical region fencing that is required.
- Cross-border data transfers will require the appropriate regulatory and legal filing.
- X-Rite, as applicable maintains all ownership rights to data hosted by a Cloud Service Providers, even while residing within the environment of a Cloud Service Providers.

12 Physical and Environmental Security

12.1 General Physical Access

- Physical access to X-Rite facilities must be controlled via electronic badge access systems, with everyone requiring access obtaining an individually assigned access badge.
- X-Rite facilities access will be restricted to individuals based on organization requirements and job function.
- Entry and exits to restricted areas must be monitored and recorded 24/7 by digital means and stored for a period of at least 90 days unless otherwise prohibited by local law. X-Rite must comply with applicable local law requirements regarding notifying associates and others of any such monitoring.
- All X-Rite visitors, contractors, and vendors are required to display badges, and must sign in and out with recorded details of the visit. Visitors must be escorted by an associate at all times.

12.2 Data Center Access

- Physical access to a data center or room and supporting utilities must always be locked and restricted to those individuals requiring access based on job duties.
- X-Rite is required to semi-annually validate the authorized entry list and ensure only authorized individuals accessed the data center.
- When access to workstations, servers or other consoles in the data center is not needed, they must be locked out or the user must logout of the system.
- A visitor log for the data center must be maintained and stored for a period of at least 90 days. Visitors must be escorted by an associate at all times.

12.3 Environmental Protections

- Temperature, humidity, water and fire controls must be implemented and maintained to ensure proper functioning of the equipment housed in the data center.
- Monitoring and alerting mechanisms must be implemented to notify facilities and/or systems administration personnel when less than optimal environmental conditions are reached in the data center.

13 Asset Management

13.1 Asset Inventory

- X-Rite shall maintain an inventory of all IT assets identifiable by their business owner, IT owner, and business criticality.
- The inventory of IT assets must be stored in a central repository, electronically searchable, reviewed, and updated on a regular basis.

13.2 Endpoint Security

- X-Rite ensures that all data on an endpoint remains encrypted while at rest and in transit.
- X-Rite maintains a patch management policy and deploys patches based on their criticality levels and timelines established in the patch management policy.
- X-Rite deploys anti-malware protection on all of its endpoints (i.e., servers, workstations, and mobile devices where possible) with a configuration so that malware and virus signatures are automatically updated, and real-time detection is enabled so that malicious software and files can be identified and quarantined as quickly as possible. Additionally, users do not have the ability to disable or adjust the policy setting of the anti-malware protection on the endpoints.
- X-Rite deploys a Data Loss Prevention (DLP) solution to prevent the unauthorized transmission or disclosure of data.
- X-Rite deploys an internet content filtering solution to restrict access to non-work related websites (i.e. social networking, personal email, data sharing).
- X-Rite implements and maintains an email content filtering mechanism to remove or quarantine incoming emails with high risk file types (such as executables).
- X-Rite logs and monitors activities at the network and host level for all systems supporting services.

14 Change and Configuration Management

- X-Rite must have a formalized and documented change management process whereby changes are formally documented and approved.
- Management approval of all changes to the production environment must be retained and auditable for 12 months.

15 Application Security

- X-Rite maintains a documented application development approach that includes security gates/practices that ensures security by design.
- X-Rite develops, implements, and maintains its applications securely so as to limit vulnerabilities and harden against common exploits and attacks.
- Secure coding standards are documented within X-Rite.
- X-Rite application source code must be stored and tracked in code versioning repositories with access restricted to associates who require access based on assigned job responsibilities.
- Code reviews, whether manual by a peer or using automated scanning tools, must be performed on all internally developed applications prior to promotion to the production environment.
- Developers and those responsible for code review shall participate in an annual secure coding training to understand and identify common coding security vulnerabilities, including but not limited to coding standards such as prohibiting the disclosure of sensitive architectural secrets in comments/header information, hard-coding of encryption keys and access credentials, avoiding the use of third party code frameworks and repositories with known vulnerabilities, and ensuring adequate security testing is performed and approved.
- X-Rite prohibits the use of production data in lower development and test environments so that data is effectively managed on a need-to-know basis and protected against improper information disclosure in accordance with the principle of least privilege.
- Access to IT production environments is restricted to personnel who require access due to assigned job duties.
- X-Rite performs application penetration tests or vulnerability scans to identify common vulnerabilities or security flaws in the application in scope for services provided.

- X-Rite develops remediation plans and track through completion all issues and findings identified during the external network vulnerability assessments/penetration tests.

16 Network

16.1 Firewalls and Network Security

- All X-Rite private networks must be separated from any non-X-Rite private network by the use of a firewall device.
- All inbound and outbound communications from the internet to X-Rite private networks must be restricted by a firewall device.
- The default firewall policy must deny all traffic except for explicitly permitted traffic with a valid business justification.
- All firewall devices must be configured to log permitted and denied traffic to a centralized log repository.
- All firewall devices must support stateful packet inspection capabilities.
- All firewall and router policy rulesets must be reviewed and updated on a semi-annual basis.
- The X-Rite network shall be segmented where applicable to prevent the spread of worms, viruses, malicious software, and unauthorized access between locations.
- When critical X-Rite business operations are performed using web applications (whether hosted by IT or in a cloud service), they must be protected by a web application firewall.
- Network intrusion detection technology is deployed to monitor and detect any abnormal network activity.

16.2 Wireless Networking

- X-Rite wireless networks and access points must be architected, installed, and maintained by the IT department.
- X-Rite wireless access points and networks must conform and not interfere to FCC maintained radio spectrum or other governing body requirements.
- X-Rite wireless networks must require authentication of the user and/or device to establish connectivity.
- X-Rite wireless networks must use the strongest vendor available cryptography and security protocols.
- X-Rite wireless network activity must be logged to a centralized log repository.
- X-Rite wireless networks must be segmented via a firewall from internal wired networks.
- Scans for rogue wireless access points must be performed quarterly to identify authorized and unauthorized access points. Unauthorized access points must be removed immediately and IT Security notified.

16.3 Guest Networks

- X-Rite guest networks must be established and implemented to permit visitors access to the internet but not permit access to any IT asset or data via firewall device.
- All inbound and outbound communications to X-Rite guest networks must be restricted and logged by a firewall device to a central logging repository.
- X-Rite guest networks need to be configured to not broadcast an SSID or require a guest to log in.

16.4 Services

- X-Rite network devices must be configured to permit the fewest ports, protocols, and services to be enabled based on business functionality requirements. The use of each port, protocol, and service must be able to be linked to an associated business/application justification.

16.5 Proxies and Web Content Filtering

- X-Rite proxies and web content filters shall be implemented to disallow access to malicious web sites based on categorization.
- X-Rite website traffic will be analyzed for malicious activity where permitted by law.
- Geo-blocking shall be implemented to restrict access to web sites in countries with whom X-Rite does not conduct business.

16.6 Minimum Security Baseline and Hardening

- Minimum security configuration baseline requirements must be documented for every X-Rite network device type.
- Network devices connecting to the X-Rite network must be hardened to and comply with the minimum-security configuration baseline requirements.

16.7 Device Time Synchronization

- Time must be synchronized with a central time source using Network Time Protocol (NTP) to ensure all X-Rite systems maintain an accurate system clock.

16.8 Remote Access

- Remote access capabilities must be provisioned anytime access to X-Rite private networks is necessary.
- Remote access over a public network such as the internet or a public wireless network must utilize encryption technology such as a virtual private network (VPN).
    - VPN devices must allow only one concurrent connection per user.
    - All VPN connections must require multi-factor authentication and terminate sessions after 24 hours.
- Personal equipment that is authorized to be used to connect to X-Rite private networks must meet minimum security baseline requirements.
- Modems providing remote access must be documented and approved.
- X-Rite issued mobile devices must have the ability to be remotely wiped (e.g., smart phones, tablets)
- IT assets must be configured to permit the fewest ports, protocols, and services to be enabled based on business functionality requirements.
- Anti-virus/Anti-malware software must be implemented on all X-Rite IT assets.
    - Malware definitions must be kept up to date.
    - Detective scans are to occur on at least a weekly basis.
    - Anti-malware software with heuristic capabilities must be used.
    - Systems not connected to the X-Rite network must be configured for automatic updates from the vendor.
    - Anti-malware software must be deployed such as to prevent disabling or removal.

17 Security Monitoring and Logging

X-Rite IT systems must be configured to log all significant successful and unsuccessful IT security events to aid in security investigations and to meet compliance requirements.

- IT Security will identify systems for log collection.
- All logs must be stored in a centralized logging repository and made available for IT security analysis.
- Logs must be analyzed for cyber threat activity daily by the Security Operations Center (SOC).

18 Vulnerability Identification and Management

18.1 Vulnerability Scanning and Assessment

- X-Rite must perform internal and external vulnerability scanning of all IT assets environment to identify and remediate identified vulnerabilities.
- Vulnerability scans must include all network segments.
- Remediation of identified vulnerabilities must be prioritized based on age and criticality of the finding in accordance to the Vulnerability Management Policy.

18.2 Security Testing

- X-Rite will coordinate security testing of relevant IT systems on an annual basis. Security test results must contain a detailed description of findings including vulnerabilities identified, evaluation of risk level, impact of threat, likelihood of exploitation, and technical recommendations.

- X-Rite is responsible for prioritizing remediation of any findings from the security test based on an impact analysis and criticality of the finding.

18.3 System Patching

- X-Rite must maintain current and up to date software and systems including vendor patches.
- Software patches must be configured to occur over the network.
- Software patches must be able to be applied based on critical business need.

19 Security Assessments and Audits

- X-Rite shall provide available external security audit reports upon request.
- X-Rite will allow security assessments or audits performed by customers or their authorized professional representative and shall provide all assistance reasonably required, provided that the customer respects the X-Rite Audit Request Process (including at least three weeks advance notice).
- X-Rite will allow a security assessment or audit once per calendar year.
- X-Rite will not be responsible for any costs associated with the security assessment or audit as performed by customers or their authorized professional representative.
- X-Rite shall remedy any identified security deficiencies which are confirmed and acknowledged and this in a timely manner.

****** END OF DOCUMENT ******