ZIMMER BIOMET

Your progress. Our promise.®

Information Security Controls

@ Zimmer Biomet

May 2018

Contact: zbs-security@zimmerbiomet.com

Table of Contents

Introduction

This document contains an overview of the Information Security controls that are in place at Zimmer Biomet, starting from the pre-screening that is done at the time of employment offer to Governance to Onboarding, and everyday IT Operations to off-boarding.

1. Governance

Zimmer Biomet's Information Security program has adopted the ISO 27001 standard for information security governance. There is an Information Security department that is led by the IT Risk and Information Security Officer who oversees the global information security program. Zimmer Biomet has a comprehensive set of policies, standards and procedures for global IT Operations.

2. Employee Pre-Screening

To facilitate hiring trustworthy individuals, Zimmer Biomet partners with a company specializing in background investigations, to conduct background checks on potential new hires in the US. The results of the screening are reviewed by the ZB HR Recruiting team to ensure compliance with hiring standards. Individuals in the US also complete a drug screen.

3. Onboarding

When a new workforce member is on-boarded, they go through the following steps in our provisioning process.

a. *Identity and Access Management*

A provisioning system is used to automatically provision, update and de-provision through Directory Services and email accounts.

Directory Services are used as the primary means for network and application access. Individuals are assigned roles according to job position and different network and application permissions are granted or restricted according to the role. If an individual needs access to a system or application beyond this, a request is created through a ticketing system and routed to the individual's supervisor for approval. Then the request is routed to the appropriate business unit for approval, and then permission is granted. Access requires a business justification.

All other third party accounts are provisioned\de-provisioned manually following standard operating procedures.

4. User Controls

a. ***Hard Disk Encryption***

Zimmer Biomet applies encryption to critical user workstations.

b. End Point Protection

Endpoints are protected with a market leading endpoint protection product. Definitions are kept current through automatic updating to ensure the latest definitions are continually pushed to the clients.

c. URL Filtering / Proxies

Web proxies are in place to protect end user assets from malicious web traffic. Web traffic from workstations is routed through the proxies to block web traffic to, and from known malicious servers as well as other harmful websites. This activity is logged and recorded in the Security Incident and Event Management (SIEM) system for event correlation as well.

d. 24X7 Help Desk

ZB maintains a 24X7 help desk to ensure employees can promptly report any potential security related issue. Response to reported issues varies based on severity of the reported event.

5. Server Controls

a. ***Build standards***

Server installation is done in accordance with internal build standards.

b. ***Regular scanning***

Client and server systems are scanned regularly through endpoint protection that is in place. In addition to anti-virus, anti-spyware and anti-malware scanning, there is recurring vulnerability scanning.

c. Patching

Patching for servers is performed as required.

6. Data Protection controls

a. Backup and Storage

Backups are done regularly and stored offsite through a service provider that specializes in data backup storage. Test recoveries are conducted quarterly to verify recovery processes are adequate, and a software solution is in place to verify data integrity of backups.

b. Fileshare protection

Fileshare access is granted based on job role. Individuals must either fill a role that requires access to a particular portion of the file share or be granted access to a file share through directory services in the same manner as they are granted access for applications.

7. Change Control Process

All changes to production follow the ZB Change Control Process. Changes are routed through the change manager to the change advisory board (CAB). In order for a change to be accepted, it must have a business justification, be properly tested, have roll back procedures in case of unforeseen difficulties, be implemented into disaster recovery plans as required, and follow proper documentation and quality control procedures.

8. External Perimeter Protection

a. Firewalls

Zimmer Biomet uses leading perimeter firewalls to protect the internal network from the external network and to protect internal networks of different trust levels.

b. Network Security and Monitoring

Load balancers are in place to ensure servers are load protected and hide their identity from outside sources. The network is highly redundant to ensure availability and network equipment is monitored around the clock using monitoring tools. System logs are sent to the Security Incident and Event Management (SIEM) system for event monitoring and correlation.

c. Security Operations Center (SOC)

Intrusion detection/prevention systems are in place to identify potential attacks or malicious payloads. SIEM provides correlation and feedback on security related events on a 24X7 basis. These events are monitored by on-site and off-site personnel for remediation actions as required.

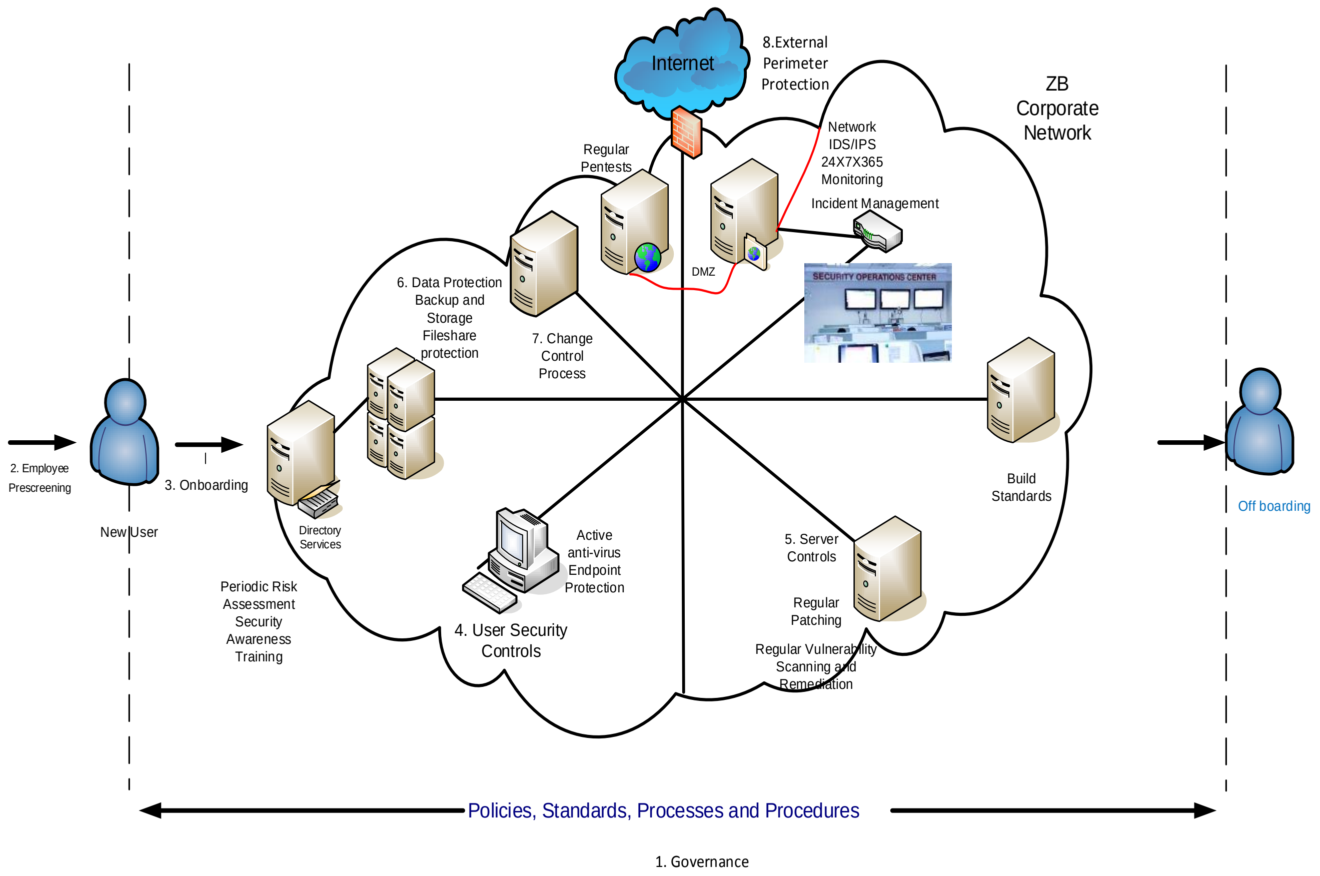
d. *Cyber Incident response*

When an incident is identified and reported through log correlation and monitoring, SOC personnel undertake triage and analysis. Incidents are also reported to the service desk by end users. Depending on the severity of the incident, a priority ticket is raised for analysis and remediation. Incidents are escalated and routed based on severity. Subsequent remedial action is taken and documented.

e. *Attack and Penetration tests, and remediation*

Penetration testing is conducted by internal and qualified third parties.

9. Graphical Representation of Controls


Internet
8.External Perimeter Protection
ZB Corporate Network
Regular Pentests
Network IDS/IPS 24X7X365 Monitoring
Incident Management
DMZ
SECURITY OPERATIONS CENTER
6. Data Protection Backup and Storage Fileshare protection
7. Change Control Process
2. Employee Prescreening
3. Onboarding
New User
Directory Services
Build Standards
Off boarding
Periodic Risk Assessment Security Awareness Training
Active anti-virus Endpoint Protection
4. User Security Controls
5. Server Controls
Regular Patching
Regular Vulnerability Scanning and Remediation
Policies, Standards, Processes and Procedures
1. Governance

10. Revision History:

Rev	Date Released	Description of Change
2	May 9, 2018	General refresh updates.
1	February 17, 2017	Initial release