Microsoft Cloud Assessment Report

NOVACOAST SCHOOL OF MINES

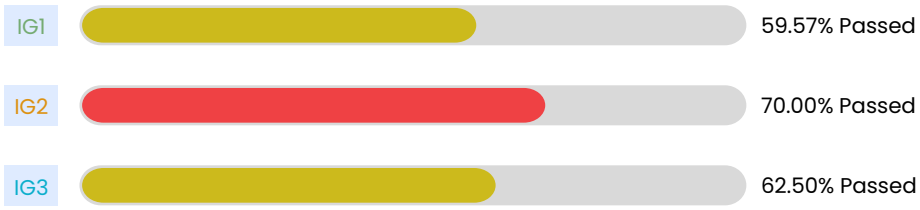
Executive Summary

Primary Domain	EntraID Sync Enabled	Primary License
novacoastschool.com	true	Microsoft 365 Business Premium

Licensed Users	Non-licensed Users	Guest Users
70	157	1

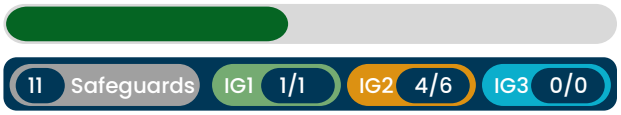
CIS Controls

**Note that the results found are limited to the automated evidence collected. You also may be using 3rd party/alternative solutions for controls that did not pass acrorss the various safeguards.



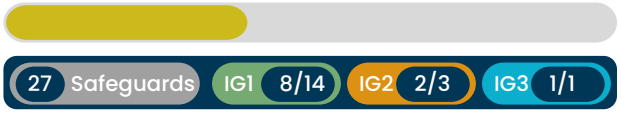
1 Inventory and Control of Enterprise Assets

2 Inventory and Control of Software Assets



3 Data Protection

4 Secure Configuration of Enterprise Assets and Software

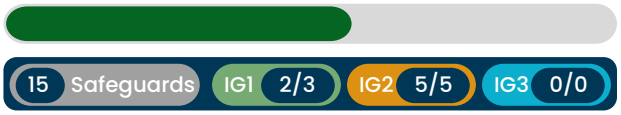


5 Account Management

6 Access Control Management

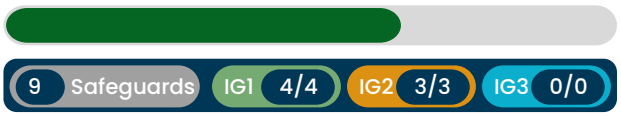
7 Continuous Vulnerability Management

8 Audit Log Management



9 Email and Web Browser Protections

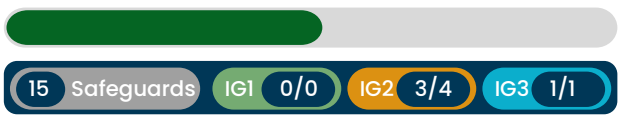
10 Malware Defenses



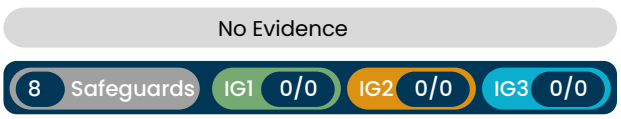
11 Data Recovery

12 Network Infrastructure Management

13 Network Monitoring and Defense



14 Security Awareness and Skills Training



15 Service Provider Management

No Evidence

16 Application Software Security

No Evidence

17 Incident Response Management

No Evidence

18 Penetration Testing

No Evidence

Table Of Contents

Security License Utilization

License	Function	Available in Tenant	Utilized	Notes
Entra ID P1	Identity Protection	🟢	🟢	At least 1 Conditional Access policy being leveraged
Entra ID P2	Advanced Identity Protection	🟢	🟠	No conditional access policy being leveraged for risky users
Intune	MDM	🟢	🟡	4 out of 10 devices are enrolled into the MDM solution
Defender for Endpoint/Defender for Business	EndPoint Protection (EDR)	🟢	🟡	2 of detected devices are seen in Defender
Defender for Office 365	Advanced Email Security	🟢	🟠	No Defender for Office 365 policies detected
Defender for Cloud Apps	Application Security	🟢	🟢	None

Users

User Health

Top Risky Users

No risk detections found for users

MFA Adoption

57 licensed Users are not enrolled in MFA and are not covered through conditional access or security defaults

Conditional Access

Is the primary method of MFA enforcement

Insights on identity attacks

The first quarter of 2023 saw a dramatic surge in password-based attacks against cloud identities, especially in the education sector.

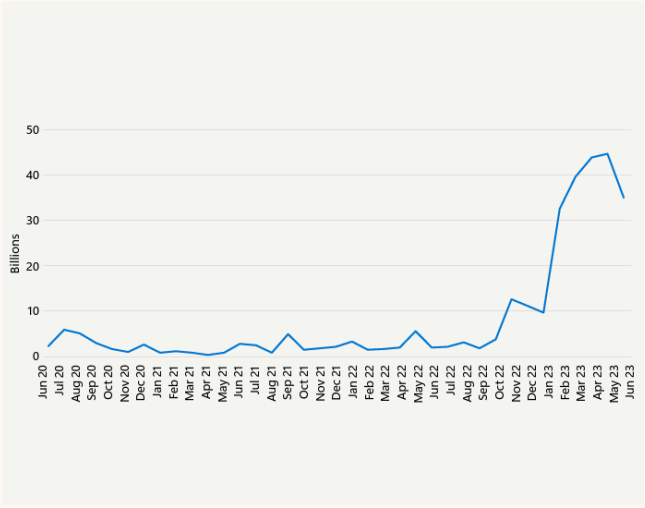
According to Microsoft Entra data, the number of attempted attacks increased more than tenfold compared to the same period in 2022, from around 3 billion per month to over 30 billion. This translates to an average of 4,000 password attacks per second targeting Microsoft cloud identities this year.

One of the main reasons password attacks are so prevalent is the low security posture of many organizations, especially in the education sector. Many of these organizations have not enabled MFA for their users, leaving them vulnerable to phishing, credential stuffing, and brute force attacks.

We blocked an average of 4,000 password attacks per second over the past year.

Password based attacks spiked in 2023

After a notable increase in the number of password-based attacks per month in October 2022, the number skyrocketed in 2023. In April, there were 11,000 attacks per second, a tenfold increase from the same time last year.



Source: Microsoft Entra data

Email

Email and Phone are considered weaker forms of MFA. Stronger methods like Microsoft Authenticator should be used.

Methods Present

Method	Strength	Phishing Resistant	Count
Email	Weak	False	19
Microsoft Authenticator	Strong	False	7
Phone	Weak	False	12
Software OAuth Token	Strong	False	1

Other Risk Factors

25 Global Admins

were deteted. This role provides rights to perform any action in a tenant. These number of the users assigned to this role should be limited to 2 but no more than 4. It is recommended to adopted Privileged Identity Mangement as part of the Entra ID P2 offering in order to reduce your attack surface and provide just in time access.

43 Dormant Accounts

were discovered. Dormant accounts increase your attack surface. Attackers leverage these accounts to gain intial access and move laterally across an organization

Devices

Device Health

10 devices detected

Windows	macOS	Android	iOS	Other
10 Devices	0 Devices	0 Devices	0 Devices	0 Devices

Managed Devices

10 Devices	2 Devices	2 Devices
Found in Active Directory	Found in Mobile Device Management	Found enrolled for endpoint protection

0

Devices discovered that are classified as personal and not enrolled into Mobile Device Management (Intune)

80-90%

of all successful ransomware compromises originate through unmanaged devices.

Active Malware cannot be detected as no devices enrolled in endpoint protection

0 Devices

Classified as compliant

2 Devices

Classified as noncompliant

Top Risky Devices

Device	User	Reason
WINDEV2311EVAL	Godzilla	Non Compliant
ALEXW-PC	Alex Wilber	Non Compliant

Mail

Email Health

61 Mailboxes Found

0 Mailboxes over 90% Full

Email Security

Domain Authentication Health		Link Protection	
Anti-phishing Policies		Attachment Protection	
Anti-spam Policies		Anti-Malware Policies	

1 Licensed Shared Mailboxes Found

Shared Mailboxes do not required a license and should be removed

Autoforwarding to external domains is Disabled

Autoforwarding should be disabled. If an adversary gains access to an account, they might set up forwarding rules to gather intelligence continuously. Disabling external auto-forwarding hinders this technique

1 Inventory and Control of Enterprise Assets

IG1

Safeguard	Microsoft Control	Evidence	Result
1.1 Establish and Maintain Detailed Asset Inventory	All Devices shall be inventoried and periodically reviewed.	10 devices are active in inventory. 2 are enrolled in Intune.	Passed
1.1 Establish and Maintain Detailed Asset Inventory	Devices shall be deleted that haven't checked in for over 30 days.	10 Devices have not checked in for 30+ days	Failed
1.2 Address Unauthorized Assets	Personal Devices should be restricted from enrolling into the MDM solution	2 Personal Devices are enrolled into Intune	Failed

IG2

Safeguard	Microsoft Control	Evidence	Result
1.3 Utilize an Active Discovery Tool	Microsoft Intune is configured for Autoenrollment	Enablement Content Link	Manual
1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	N/A	N/A	N/A

IG3

Safeguard	Microsoft Control	Evidence	Result
1.5 Use a Passive Asset Discovery Tool	Azure AD Audit logs are periodically reviewed to identify assets trying to access the network	Azure AD Logs are being Collected See All Evidence	Passed

2 Inventory and Control of Software Assets

IG1

Safeguard	Microsoft Control	Evidence	Result
2.1 Establish and Maintain a Software Inventory	All corporate approved applications are cataloged and periodically reviewed	26 Enterprise applications were detected. See All Evidence	Passed
2.2 Ensure Authorized Software is Currently Supported	The vulnerability management dashboard is periodically reviewed	Manual Enablement Content Link	Manual
2.3 Address Unauthorized Software	Unsanctioned Applications are blocked	Manual Enablement Content Link	Manual
2.3 Address Unauthorized Software	Configure a Next-Generation policy that protects against potentially unwanted apps (PUA)	Manual Enablement Content Link	Manual

IG2

Safeguard	Microsoft Control	Evidence	Result
2.4 Utilize Automated Software Inventory Tools	Cloud App Discovery is configured and apps are periodically reviewed	Your tenant is licensed for Defender for Cloud Apps	Passed
2.5 Allowlist Authorized Software	Only Admins shall be allowed to register 3rd party applications	Secure Score Controls Enablement Content Link	Failed
2.5 Allowlist Authorized Software	Only Approved Apps SHOULD Be Installed	Third party apps and custom apps should be restricted in the Teams App PolicySee All Evidence	Failed
2.5 Allowlist Authorized Software	Mobile devices shall only be able to access corporate data through approved client apps	A conditional Access policy exist that supports this control See All Evidence	Passed
2.5 Allowlist Authorized Software	Authorized Applications should be deployed to managed devices	Applications are being deployed through Intune See All Evidence	Passed
2.6 Allowlist Authorized Libraries	Attack Surface Reduction rules shall be configured	Attack surface reduction policy found in Intune See All Evidence	Passed

IG3

Safeguard	Microsoft Control	Evidence	Result
2.7 Allowlist Authorized Scripts	Users SHALL Be Prevented from Running Custom Scripts	Enablement Content Link	Manual

3 Data Protection

IG1

Safeguard	Microsoft Control	Evidence	Result
3.1 Establish and Maintain a Data Management Process	A data management process is defined for Teams, SharePoint, and OneDrive	Manual	Manual
3.2 Establish and Maintain a Data Inventory	Teams/Teams Channels are documented and periodically reviewed	Teams Channels were discovered See All Evidence	Manual
3.2 Establish and Maintain a Data Inventory	Teams/Teams channel creation is restricted	Manual Enablement Content Link	Manual
3.2 Establish and Maintain a Data Inventory	SharePoint Sites are documented and Periodically reviewed	SharePoint sites were discovered. See All Evidence	Manual
3.3 Configure Data Access Control Lists	Groups are inventoried and periodically reviewed for data access	Groups were discovered. See All Evidence	Manual
3.3 Configure Data Access Control Lists	Non-admin users shall be prevented from providing consent to 3rd party applications	Secure Score Controls. Enablement Content Link	Failed

Safeguard	Microsoft Control	Evidence	Result
3.3 Configure Data Access Control Lists	File and Folder Links Default Sharing Settings SHALL Be Set to "Specific People	Manual. Enablement Content Link	Manual
3.3 Configure Data Access Control Lists	External sharing SHOULD be limited to approved domains and security groups per interagency collaboration needs.	Secure Score Controls.	Passed
3.4 Enforce Data Retention	Retention Policies shall be configured	Manual. Enablement Content Link	Manual
3.5 Securely Dispose of Data	Groups are set up for expiration	Manual. Enablement Content Link	Manual
3.5 Securely Dispose of Data	Teams channels are set up for expiration due to inactivity	Manual. Enablement Content Link	Manual
3.6 Encrypt Data on End-User Devices	Encryption shall be required on all devices	2 were found that are not encrypted. See All Evidence	Failed

IG2

Safeguard	Microsoft Control	Evidence	Result
3.7 Establish and Maintain a Data Classification Scheme	Information Protection Labels shall be configured	Secure Score Controls. Enablement Content Link	Passed
3.8 Document Data Flows	Teams/Teams Channels are documented and periodically reviewed	Teams Channels were discovered. See All Evidence	Manual
3.9 Encrypt Data on Removable Media	Configure an endpoint protection configuration profile for removeable data drives	Manual. Enablement Content Link	Manual
3.11 Encrypt Sensitive Data at Rest	N/A	"Data is encrypted at rest by default". Enablement Content Link	Manual
3.12 Segment Data Processing and Storage Based on Sensitivity	Private and Shared Channels shall be utilized to restrict access to sensitive information	0 Private channels discovered See All Evidence	Failed
3.12 Segment Data Processing and Storage Based on Sensitivity	Sensitive SharePoint Sites SHOULD Adjust Their Default Sharing Settings to Those Best Aligning to Their Sensitivity Level	Manual. Enablement Content Link	Manual

IG3

Safeguard	Microsoft Control	Evidence	Result
3.13 Deploy a Data Loss Prevention Solution	Data loss prevention policies shall be configured	Secure Score Controls. Enablement Content Link	Passed

4 Secure Configuration of Enterprise Assets and Software

IG1

Safeguard	Microsoft Control	Evidence	Result
4.1 Establish and Maintain a Secure Configuration Process	External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings	Teams Policy configured accurately. See All Evidence	Passed
4.1 Establish and Maintain a Secure Configuration Process	Anonymous Users SHALL NOT Be Enabled to Start Meetings	Teams Policy configured accurately. See All Evidence	Passed
4.1 Establish and Maintain a Secure Configuration Process	Automatic Admittance to Meetings SHOULD Be Restricted	Teams Policy misconfigured. See All Evidence	Failed
4.1 Establish and Maintain a Secure Configuration Process	Unmanaged users SHALL NOT be enabled to initiate contact with internal users.	Teams Policy misconfigured. See All Evidence	Failed
4.1 Establish and Maintain a Secure Configuration Process	Contact with Skype Users SHALL Be Blocked.	Teams Policy configured accurately. See All Evidence	Passed
4.1 Establish and Maintain a Secure Configuration Process	Security Baselines should be configured for Windows Devices	Security Baseline policy configured. See All Evidence	Passed
4.1 Establish and Maintain a Secure Configuration Process	Devices compliance policies shall be configured for every supported device platform	Device Compliance policies discovered. See All Evidence	Passed
4.1 Establish and Maintain a Secure Configuration Process	Devices compliance policies shall be configured for every supported device platform	Manual. Enablement Content Link	Manual
4.1 Establish and Maintain a Secure Configuration Process	Compliance Policies are configured to incorporate Defender settings	Manual. Enablement Content Link	Manual
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	Automatic forwarding to external domains SHALL be disabled	No transport rule found.	Failed
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	External sender warnings SHALL be implemented.	Manual. Enablement Content Link	Manual
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	Ensure mail transport rules do not whitelist specific domains	No transport rules whitelisting domains.	Passed
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	Inbound Anti-Spam Protections SHALL Be Enabled.	No Anti-spam policy found.	Failed
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	IP Allow Lists SHOULD NOT be Implemented.	IP Allow list discovered.	Passed
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	Lockout screen and password settings shall be configured for each device.	Secure Score Controls. Enablement Content Link	Failed
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	Browser Sessions shall not be persistent for privileged users	No conditional access policy found. See All Evidence	Failed

Safeguard	Microsoft Control	Evidence	Result
4.4 Implement and Manage a Firewall on Servers	N/A	N/A	N/A
4.5 Implement and Manage a Firewall on End-User Devices	Browser Sessions shall not be persistent for privileged users	Windows Firewall policy found in Intune. See All Evidence	Passed
4.6 Securely Manage Enterprise Assets and Software	N/A	N/A	N/A
4.7 Manage Default Accounts on Enterprise Assets and Software	Highly privileged role assignments shall be periodically reviewed	Manual. Enablement Content Link	Manual

IG2

Safeguard	Microsoft Control	Evidence	Result
4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Legacy Authentication shall be blocked	Conditional Access Policy found See All Evidence	Passed
4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	File Sharing and File Storage Options shall be blocked	3rd party file sharing is blocked in Teams	Failed
4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Calendar and Contact Sharing SHALL Be Restricted	Secure Score Controls. Enablement Content Link	Passed
4.9 Configure Trusted DNS Servers on Enterprise Assets	N/A	N/A	N/A
4.10 Enforce Automatic Device Lockout on Portable End-User Devices	Lockout screen and password settings shall be configured for each device	Manual Enablement Content Link	Manual
4.11 Enforce Remote Wipe Capability on Portable End-User Devices	Devices and Applications shall be wiped when a user leaves the organization or reports a lost/stolen device	Manual Enablement Content Link	Manual

IG3

Safeguard	Microsoft Control	Evidence	Result
4.12 Separate Enterprise Workspaces on Mobile End-User Devices	App Protection policies should be created for mobile devices	Polices are in Intune for iOS and Android See All Evidence	Passed

5 Account Management

IG1

Safeguard	Microsoft Control	Evidence	Result
5.1 Establish and Maintain an Inventory of Accounts	An inventory of accounts in Active directory is periodically reviewed	Manual. See All Evidence	Manual

Safeguard	Microsoft Control	Evidence	Result
5.1 Establish and Maintain an Inventory of Accounts	Highly privileged role assignments shall be periodically reviewed Evidence	Manual. See All Evidence	Manual
5.2 Use Unique Passwords	Passwords shall not expire	Secure Score Controls. Enablement Content Link	Passed
5.3 Disable Dormant Accounts	Dormant accounts are disabled after 45 days	90 accounts were found active that have not signed in for over 45 days. See All Evidence	Failed
5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts	The number of users with highly privileged roles shall be limited Evidence	25 Global admin were detected. See All Evidence	Failed
5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts	Highly privileged accounts shall be cloud-only	All Global Admins are cloud-only. See All Evidence	Passed

IG2

Safeguard	Microsoft Control	Evidence	Result
5.5 Establish and Maintain an Inventory of Service Accounts	An inventory of service accounts in Active directory is periodically reviewed	Manual. See All Evidence	Manual
5.6 Centralize Account Management	Corporate applications are configured for SCIM provisioning	Manual. Enablement Content Link	Manual

6 Access Control Management

IG1

Safeguard	Microsoft Control	Evidence	Result
6.1 Establish an Access Granting Process	Guest users have limited access to properties and memberships of directory objects	Manual. Enablement Content Link	Manual
6.1 Establish an Access Granting Process	Dynamic Groups are leveraged for automated group management	Dynamic Group(s) detected. See All Evidence	Passed
6.1 Establish an Access Granting Process	A formal process is in place for users to request guest access	Manual. Enablement Content Link	Manual
6.1 Establish an Access Granting Process	Users assigned highly privileged roles shall not have permanent permissions	ManualEnablement Content Link	Manual
6.1 Establish an Access Granting Process	Activation of privileged roles should be monitored and require approval	Manual. Enablement Content Link	Manual
6.1 Establish an Access Granting Process	Managed Devices shall be required for authentication	1 Conditional Access Policy found: Managed Devices shall be required for authentication. See All Evidence	Passed

Safeguard	Microsoft Control	Evidence	Result
6.1 Establish an Access Granting Process	External User Access SHALL Be Restricted	Teams Policy misconfigured. See All Evidence	Failed
6.2 Establish an Access Revoking Process	Guest access is periodically reviewed and access is removed if there is no longer any collaboration	Dormant guest users discovered. See All Evidence	Failed
6.2 Establish an Access Revoking Process	Expiration times for 'guest access to a site or OneDrive' and 'people who use a verification code' SHOULD be set to 30 days	Manual. Enablement Content Link	Manual
6.2 Establish an Access Revoking Process	Expiration Date SHOULD Be Set for Anyone Links	Manual. Enablement Content Link	Manual
6.3 Require MFA for Externally-Exposed Applications	MFA is enforced for all users	A conditional access policy is either missing or misconfigured. See All Evidence	Failed
6.3 Require MFA for Externally-Exposed Applications	MFA is enforced for Azure Management	Conditional Access Policy found that enables MFA for Azure Management. See All Evidence	Passed
6.4 Require MFA for Remote Network Access	MFA shall be required to enroll devices to Azure AD	A conditional access policy is either missing or misconfigured. See All Evidence	Failed
6.4 Require MFA for Remote Network Access	A conditional access policy is enabled which requires guest users to use MFA	A conditional access policy is either missing or misconfigured. See All Evidence	Failed
6.4 Require MFA for Remote Network Access	MFA Shall be required for Intune Enrollment	A conditional access policy is either missing or misconfigured. See All Evidence	Failed
6.5 Require MFA for Administrative Access	MFA is enforced on accounts with highly privileged roles	Conditional Access Policy found that enforcing MFA for admins. See All Evidence	Passed

IG2

Safeguard	Microsoft Control	Evidence	Result
6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems	Windows Hello for Business should be configured where applicable Evidence	A configuration is either missing or misconfigured. See All Evidence	Failed
6.7 Centralize Access Control	Authorized Applications shall be configured for Single Sign-On	SSO Apps were found. See All Evidence	Passed

IG3

Safeguard	Microsoft Control	Evidence	Result
6.8 Define and Maintain Role-Based Access Control	Highly privileged role assignments shall be periodically reviewed	Manual. Global Admins found. See All Evidence	Manual

Safeguard	Microsoft Control	Evidence	Result
6.8 Define and Maintain Role-Based Access Control	Only users with the Guest Inviter Role are allowed to invite external users	Manual. Enablement Content Link	Manual

7 Continuous Vulnerability Management

IG1

Safeguard	Microsoft Control	Evidence	Result
7.1 Establish and Maintain a Vulnerability Management Process	A vulnerability management process is defined for Microsoft Defender and Entra ID	Manual. Enablement Content Link	Manual
7.2 Establish and Maintain a Remediation Process	A remediation process is defined for vulnerabilities detected in Microsoft Defender	Manual. Enablement Content Link	Manual
7.3 Perform Automated Operating System Patch Management	Windows Update Rings shall be configured for Windows Devices	Windows update policy found in Intune. See All Evidence	Passed
7.3 Perform Automated Operating System Patch Management	Update Policies shall be configured for Apple Devices	Update policy found in Intune. See All Evidence	Passed
7.4 Perform Automated Application Patch Management	Authorized Applications should be deployed and updated on managed devices	Applications found in Intune. See All Evidence	Passed

IG2

Safeguard	Microsoft Control	Evidence	Result
7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets	The vulnerability management dashboard is periodically reviewed	Manual. Enablement Content Link	Manual
7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Secure Score Recommendations shall be monitored and implemented	Secure Score: 51.67%. See All Evidence	Manual
7.7 Remediate Detected Vulnerabilities	Remediation steps are acted upon between Microsoft Defender and Microsoft Intune	Manual. Enablement Content Link	Manual

8 Audit Log Management

IG1

Safeguard	Microsoft Control	Evidence	Result
8.1 Establish and Maintain an Audit Log Management Process	Define an audit log retention and review process	Manual. Enablement Content Link	Manual
8.2 Collect Audit Logs	Audit Logging SHALL Be Enabled	Audit Logging Enabled.	Passed
8.2 Collect Audit Logs	Mailbox Auditing SHALL Be Enabled	Mailbox Logging not Enabled.	Failed

Safeguard	Microsoft Control	Evidence	Result
8.2 Collect Audit Logs	Azure AD Logs shall be collected	Audit Logs being collected. See All Evidence	Passed
8.3 Ensure Adequate Audit Log Storage	N/A	N/A	N/A

IG2

Safeguard	Microsoft Control	Evidence	Result
8.4 Standardize Time Synchronization	N/A	N/A	N/A
8.5 Collect Detailed Audit Logs	Azure AD Logs shall be collected	Audit Logs being collected. See All Evidence	Passed
8.6 Collect DNS Query Audit Logs	Devices shall be enrolled for Defender for Business or Defender for Endpoint	Devices found enrolled in Defender.	Passed
8.7 Collect URL Request Audit Logs	Devices shall be enrolled for Defender for Business or Defender for Endpoint	Devices found enrolled in Defender.	Passed
8.8 Collect Command-Line Audit Logs	Devices shall be enrolled for Defender for Business or Defender for Endpoint	Devices found enrolled in Defender.	Passed
8.9 Centralize Audit Logs	Microsoft Sentinel shall be configured to ingest log information	Manual.	Manual
8.10 Retain Audit Logs	Azure AD Logs shall be collected	Audit Logs being collected. See All Evidence	Passed
8.11 Conduct Audit Log Reviews	Ensure the spoofed domains report is reviewed weekly	Manual. Enablement Content Link	Manual
8.11 Conduct Audit Log Reviews	Reported phishing or suspicious emails messages are periodically reviewed	Manual. Enablement Content Link	Manual

IG3

Safeguard	Microsoft Control	Evidence	Result
8.12 Collect Service Provider Logs	Periodically Review audit logs for Guest Users and Service Principals	Manual. Enablement Content Link	Manual

9 Email and Web Browser Protections

IG1

Safeguard	Microsoft Control	Evidence	Result
9.1 Ensure Use of Only Fully Supported Browsers and Email Clients	Mobile devices shall only be able to access corporate data through approved client apps	Conditional access policy found for this control See All Evidence	Passed

Safeguard	Microsoft Control	Evidence	Result
9.2 Use DNS Filtering Services	Web Content filtering shall be configured	Manual Enablement Content Link	Manual

IG2

Safeguard	Microsoft Control	Evidence	Result
9.3 Maintain and Enforce Network-Based URL Filters	Web Content filtering shall be configured	Manual Enablement Content Link	Manual
9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Microsoft Edge Policies are configured and enforced	Manual Enablement Content Link	Manual
9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Unnecessary browser extensions are blocked with Microsoft Defender Evidence	Manual Enablement Content Link	Manual
9.5 Implement DMARC	DMARC is configured for every custom domain	DMARC not configured for primary domain	Failed
9.5 Implement DMARC	An SPF policy(s) that designates approved IPs is published	SPF not configured for primary domain	Failed
9.5 Implement DMARC	DKIM is configured for every custom domain	DKIM Not enabled for primary domain	Failed
9.6 Block Unnecessary File Types	A common attachment filter is in place to prevent certain files from being sent to end users over email	Anti-malware policy found with Common Attachment filter enabled	Passed

IG3

Safeguard	Microsoft Control	Evidence	Result
9.7 Deploy and Maintain Email Server Anti-Malware Protections	Zero-hour auto purge (ZAP) for malware SHOULD be enabled in the default antimalware policy and in all existing custom policies.	Anti-malware policy found with Zap Enabled	Passed
9.7 Deploy and Maintain Email Server Anti-Malware Protections	Safe Attachments SHALL Be Enabled	No active Safe Attachment policy found	Failed
9.7 Deploy and Maintain Email Server Anti-Malware Protections	Ensure Priority account Protection is enabled and configured	No antiphishing policy with targeted user protection found	Failed
9.7 Deploy and Maintain Email Server Anti-Malware Protections	Phishing Protections SHOULD Be Enabled	No antiphishing policy with targeted user protection found	Failed

10 Malware Defenses

IG1

Safeguard	Microsoft Control	Evidence	Result

Safeguard	Microsoft Control	Evidence	Result
10.1 Deploy and Maintain Anti-Malware Software	Microsoft Defender Antivirus is deployed through Microsoft Defender	Microsoft Defender Antivirus Policy Found. See All Evidence	Passed
10.1 Deploy and Maintain Anti-Malware Software	Safe Links policies are configured	Safe Links Policy Found.	Passed
10.2 Configure Automatic Anti-Malware Signature Updates	Security Baselines should be configured for Windows Devices	Security Baseline policy configured in Intune. See All Evidence	Passed
10.3 Disable Autorun and Autoplay for Removable Media	Security Baselines should be configured for Windows Devices	Security Baseline policy configured in Intune. See All Evidence	Passed

IG2

Safeguard	Microsoft Control	Evidence	Result
10.4 Configure Automatic Anti-Malware Scanning of Removable Media	Security Baselines should be configured for Windows Devices	Security Baseline policy configured in Intune. See All Evidence	Passed
10.5 Enable Anti-Exploitation Features	Attack Surface Reduction rules shall be configured	Attack Surface reduction policy configured in Intune. See All Evidence	Passed
10.5 Enable Anti-Exploitation Features	Controlled Folder Access Shall be configured	Manual. Enablement Content Link	Manual
10.6 Centrally Manage Anti-Malware Software	Microsoft Defender Antivirus is deployed and managed through Microsoft Intune	Microsoft Defender Antivirus policy configured in Intune. See All Evidence	Passed
10.7 Use Behavior-Based Anti-Malware Software	Real-Time behavior monitoring is enabled for Next-Gen Protection policies	Manual. Enablement Content Link	Manual

11 Data Recovery

IG1

Safeguard	Microsoft Control	Evidence	Result
11.1 Establish and Maintain a Data Recovery Process	Enterprise state roaming shall be configured for Windows devices	Manual Enablement Content Link	Manual
11.1 Establish and Maintain a Data Recovery Process	Define a data recovery process for data repositories	Manual	Manual
11.2 Perform Automated Backups	Configure Microsoft 365 Backup Policies	ManualEnablement Content Link	Manual
11.3 Protect Recovery Data	Retention Policies shall be configured	Manual Enablement Content Link	Manual
11.4 Establish and Maintain an Isolated Instance of Recovery Data	Maintain 3rd party backups of Microsoft 365 data	Manual	Manual

IG2

Safeguard	Microsoft Control	Evidence	Result
11.5 Test Data Recovery	N/A	N/A	N/A

12 Network Infrastructure Management

IG1

Safeguard	Microsoft Control	Evidence	Result
12.1 Ensure Network Infrastructure is Up-to-Date	Authorized Applications should be deployed and updated on managed devices	Applications being deployed in Intune	Passed
12.1 Ensure Network Infrastructure is Up-to-Date	MFA registration and usage shall be periodically reviewed	Manual Enablement Content Link	Manual

IG2

Safeguard	Microsoft Control	Evidence	Result
12.2 Establish and Maintain a Secure Network Architecture	Network access via Conditional Access is documented and periodically reviewed	Manual Enablement Content Link	Manual
12.3 Securely Manage Network Infrastructure	Conditional Access Policies are configured for access controls	10 Conditional Access policies found	Passed
12.4 Establish and Maintain Architecture Diagram(s)	Conditional Access Policies are configured for access controls	Manual Enablement Content Link	Manual
12.5 Centralize Network Authentication, Authorization, and Auditing (AAA)	Leverage Entra ID as your primary IDP	Manual Enablement Content Link	Manual
12.6 Use of Secure Network Management and Communication Protocols	Leverage Entra ID as your primary IDP for authentication and SSO	Manual Enablement Content Link	Manual
12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Global Secure Access is configured as needed	Manual Enablement Content Link	Manual

IG3

Safeguard	Microsoft Control	Evidence	Result
12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work	N/A	N/A	Manual

13 Network Monitoring and Defense

IG2

Safeguard	Microsoft Control	Evidence	Result

Safeguard	Microsoft Control	Evidence	Result
13.1 Centralize Security Event Alerting	Microsoft Sentinel shall be configured to ingest log information	Manual Enablement Content Link	Manual
13.1 Centralize Security Event Alerting	Incidents and Alerts are triaged in the Defender admin center	Manual Enablement Content Link	Manual
13.2 Deploy a Host-Based Intrusion Detection Solution	Devices shall be enrolled for Defender for Business or Defender for Endpoint	2 enrolled in Defender	Manual
13.3 Deploy a Network Intrusion Detection Solution	Devices shall be enrolled for Defender for Business or Defender for Endpoint	2 enrolled in Defender	Manual
13.3 Deploy a Network Intrusion Detection Solution	High Risk Users Shall Be Blocked	Conditional Access Policy found	Passed
13.3 Deploy a Network Intrusion Detection Solution	Safe Links and Safe Attachment policies are configured	Safe Link and Safe Attachment policy found	Passed
13.4 Perform Traffic Filtering Between Network Segments	Global Secure Access is configured as needed	Manual Enablement Content Link	Manual
13.5 Manage Access Control for Remote Assets	Noncompliant devices shall be blocked from accessing corporate resources.	Conditional Access Policy found	Passed
13.5 Manage Access Control for Remote Assets	OneDrive Client SHALL Be Restricted to corporate owned devices	Secure Score Controls. Enablement Content Link	Failed
13.6 Collect Network Traffic Flow Logs	Devices shall be enrolled for Defender for Business or Defender for Endpoint	2 enrolled in Defender	Manual

IG3

Safeguard	Microsoft Control	Evidence	Result
13.7 Deploy a Host-Based Intrusion Prevention Solution	Devices shall be enrolled for Defender for Business or Defender for Endpoint	2 enrolled in Defender	Manual
13.8 Deploy a Network Intrusion Prevention Solution	Devices shall be enrolled for Defender for Business or Defender for Endpoint	2 enrolled in Defender	Manual
13.9 Deploy Port-Level Access Control	Conditional Access Policies are configured for access controls	10 Conditional Access policies found	Passed
13.10 Perform Application Layer Filtering	Entra ID Application Proxy is configured for on-premise applications	Manual Enablement Content Link	Manual
13.11 Tune Security Event Alerting Thresholds	Incidents and Alerts are triaged in the Defender admin center	Manual Enablement Content Link	Manual

14 Security Awareness and Skills Training

IG1

Safeguard	Microsoft Control	Evidence	Result
14.1 Establish and Maintain a Security Awareness Program	N/A	N/A	Manual
14.2 Train Workforce Members to Recognize Social Engineering Attacks	Attack simulations shall be periodically conducted	Manual Enablement Content Link	Manual
14.4 Train Workforce on Data Handling Best Practices	N/A	N/A	Manual
14.5 Train Workforce Members on Causes of Unintentional Data Exposure	N/A	N/A	Manual
14.6 Train Workforce Members on Recognizing and Reporting Security Incidents	Microsoft Report Message or the Report Phishing add-ins shall be installed	Manual Enablement Content Link	Manual
14.7 Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	N/A	N/A	Manual
14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	N/A	N/A	Manual

IG2

Safeguard	Microsoft Control	Evidence	Result
14.9 Conduct Role-Specific Security Awareness and Skills Training	Attack simulations shall be periodically conducted	Manual Enablement Content Link	Manual

15 Service Provider Management

Service providers are often integrated with Microsoft 365 and can be seen in the enterprise applications section of Entra ID. There is no automated evidence collection for this CIS Control at this time.

16 Application Software Security

This control is related to the internal development and maintenance of 3rd party software so it is excluded.

17 Incident Response Management

This control and subsequent safeguards will vary depending on the organizations size, maturity, and risk tolerance. There is no blanket level controls in Microsoft 365 to provide.

18 Penetration Testing

Penetration testing could be performed against your Microsoft 365 environment including security assessments that identify weakness across assets such as users, applications, or devices. There are no specific Microsoft 365 controls to provide

Appendix: Evidence

Licenses

Summary

Subscription Count	Total Unused Licenses	Next Subscription Renewal
20	392	4/1/2024

License Data Set

Name	Total Qty	Unused	Renewal Date	isTrial
Privacy Management - subject rights request (50)	1	1	5/2/2024	True
Privacy Management risk	1	1	5/2/2024	True
Microsoft Defender for Endpoint P2_XPLAT	5	0	2/24/2025	False
Dynamics 365 Team Members	3	3	1/12/2025	False
Office 365 E3	35	35	4/21/2024	False
Microsoft Power Automate Free	10000	9993	-	False
Microsoft Teams Phone Standard	10	10	4/25/2024	False
Microsoft Teams Phone Resource Account	1	0	3/14/2025	False
Power Virtual Agents Viral Trial	10000	9998	-	False
Microsoft 365 Business Premium	189	153	4/1/2024	False
Exchange Online (Plan 1)	42	26	10/12/2024	False
Microsoft 365 Business Standard	121	121	4/3/2024	False
Microsoft Cloud App Security	5	1	10/23/2024	False
Microsoft 365 E5	17	14	11/15/2024	False
Microsoft Defender for Identity	5	4	1/24/2025	False
Microsoft 365 Audio Conferencing	3	3	4/27/2024	False
Azure Active Directory Premium P1	10	5	4/18/2024	False
Rights Management Service Basic Content Protection	1	1	-	False

Name	Total Qty	Unused	Renewal Date	isTrial
Microsoft 365 Business Basic	16	9	4/28/2024	False
Exchange Online (Plan 2)	8	8	4/12/2024	False

MFA Registration

Summary

Licensed Users without MFA Coverage	Primary MFA Enforcement
57	Conditional Access

MFA Registration

The following users are not registered or covered for MFA

User	Account Enabled	Licensed	Type	MFA Registered	Covered By Conditional Access	Covered by Security Defaults
Aaron Schuetz	true	true	User	false	false	false
Adele Adams	true	true	User	false	false	false
Adrian Clifford	true	true	User	false	false	false
Alex Core	true	true	User	false	false	false
Alex Lavermicocca	true	true	User	false	false	false
Andrew Scott	true	true	User	false	false	false
Anna Rasmussen	true	true	User	false	false	false
Anthony Camacho	true	true	User	false	false	false
Anthony Jennings	true	true	User	false	false	false
Ben Burns	true	true	User	false	false	false
Ben Eichholz	true	true	User	false	false	false
Brigit Sviontek	true	true	User	false	false	false
Cherry Test	true	true	User	false	false	false
Cliff Graham	true	true	User	false	false	false
Daisy Pike	true	true	User	false	false	false

User	Account Enabled	Licensed	Type	MFA Registered	Covered By Conditional Access	Covered by Security Defaults
Darryn McGuire	true	true	User	false	false	false
Dylan Feske	true	true	User	false	false	false
Ebraheem	true	true	User	false	false	false
Elliot Seeto	true	true	User	false	false	false
Eric Mink	true	true	User	false	false	false
Girma-Selassie Tsega	true	true	User	false	false	false
Girma-Selassie Tsega	true	true	User	false	false	false
Godzilla	true	true	User	false	false	false
Gradient API	true	true	User	false	false	false
Grant Sheridan	true	true	User	false	false	false
Harald Nuij	true	true	User	false	false	false
Henk Feenstra	true	true	User	false	false	false
Jake Smith	true	true	User	false	false	false
James Bergl	true	true	User	false	false	false
Janka Mihalik	true	true	User	false	false	false
Jennifer Bridges	true	true	User	false	false	false
Jennifer Evans	true	true	User	false	false	false
Jim Thorton	true	true		false	false	false
Jimmy John	true	true	User	false	false	false
John Finn	true	true	User	false	false	false
Johnathan Cox	true	true	User	false	false	false
Jolle Klos	true	true	User	false	false	false
Jose Garcia	true	true	User	false	false	false
Keith Gard	true	true	User	false	false	false
Kelechi Olelewe	true	true	User	false	false	false
Kyle Menosky	true	true	User	false	false	false

User	Account Enabled	Licensed	Type	MFA Registered	Covered By Conditional Access	Covered by Security Defaults
Lisa Varilek	true	true	User	false	false	false
Marcel Kous	true	true	User	false	false	false
Matthew Davenport	true	true	User	false	false	false
Monica Lam He	true	true	User	false	false	false
Nick Ross	true	true	User	false	false	false
Nick Ross	true	true	User	false	false	false
Ole Andersen	true	true	User	false	false	false
Pasha Volchak	true	true	User	false	false	false
Paul Torres	true	true	User	false	false	false
Peter Gerhardt	true	true	User	false	false	false
Sara Feeny	true	true	User	false	false	false
Sheri Summers	true	true		false	false	false
Susan Bihher	true	true		false	false	false
Tony Fiorentin	true	true		false	false	false
Tyler Stromberg	true	true	User	false	false	false
Wes Johnson	true	true	User	false	false	false

Users

Summary

Licensed Users	Global Admins	Guest Users	Users Not signed in for 45+ Days	Disabled Users with a License
70	25	1	90	1

Users have not signed in for over 45 days

Name	Email	Type	Role	License	Days Since Last Login
Aaron Schuetz	aschuetz@novacoastschool.com	Member	None	Microsoft 365 Business Premium	1054

Name	Email	Type	Role	License	Days Since Last Login
Adele Adams	AdeleV@novacoastschool.com	Member	None	Microsoft 365 Business Premium	161
Admin	admin@M365EDU660802.onmicrosoft.com	Member	Global Administrator	Microsoft Defender for Endpoint P2_XPLAT, Azure Active Directory Premium P1	104
Ahron Black	ablack@novacoastschool.com	Member	None	None	1054
Alex Core	acore@novacoastschool.com	Member	Global Administrator	Microsoft 365 Business Premium	585
Alex Wilber	AlexW@novacoastschool.com	Member	None	Microsoft Cloud App Security, Microsoft Power Automate Free, Microsoft Defender for Endpoint P2_XPLAT, Microsoft 365 Business Premium	320
Andrew Scott	ascott@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Anna Rasmussen	arasmussen@novacoastschool.com	Member	None	Microsoft 365 Business Premium	870
Anthony Camacho	acamacho@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Anybody Nobody	-	Member	None	None	730
Austin Hampton	-	Member	Global Administrator	None	1137
Ben Eichholz	beichholz@novacoastschool.com	Member	None	Exchange Online (Plan 1)	1137
Brigit Sviontek	bsviontek@novacoastschool.com	Member	None	Microsoft 365 Business Premium	947
Cara Coleman	CaraC@M365EDU660802.OnMicrosoft.com	Member	None	None	1138
Caroline Appleby	cappleby@novacoastschool.com	Member	None	None	1053
Chelsea Polak	cpolak@novacoastschool.com	Member	None	None	1054
Chester Bubba	cbubba@M365EDU660802.onmicrosoft.com	Member	None	None	1123
Chloe Moreau-Carrera	cMoreauCarrera@novacoastschool.com	Member	None	None	927

Name	Email	Type	Role	License	Days Since Last Login
Cliff Graham	cgraham@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Daisy Pike	dpike@novacoastschool.com	Member	None	Microsoft 365 Business Premium	948
Darryn McGuire	dmcguire@novacoastschool.com	Member	None	Exchange Online (Plan 1)	799
Delbert McCray	DelbertM@M365EDU660802.OnMicrosoft.com	Member	None	None	1138
Douglas Cothran	DouglasC@M365EDU660802.OnMicrosoft.com	Member	None	None	1136
Dustin Bastin	dbastin@novacoastschool.com	Member	None	None	1229
Dylan Feske	dfeske@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Elliot Eliason	-	Member	None	None	1137
Elliot Seeto	eseeto@novacoastschool.com	Member	None	Microsoft 365 Business Basic	527
Eric Mink	emink@novacoastschool.com	Member	None	Microsoft 365 Business Premium	946
Ethan Milner	emilner@novacoastschool.com	Member	None	Microsoft 365 Business Premium	842
Fatima Zapata	FatimaZ@M365EDU660802.OnMicrosoft.com	Member	None	None	1144
Geraldine Fricke	gfricke@novacoastschool.com	Member	None	Microsoft 365 Business Premium	764
Girma-Selassie Tsega	girmaselassietsegay@novacoastschool.com	Member	Global Reader	Microsoft 365 Business Premium	550
Girma-Selassie Tsega	gtsegay@novacoastschool.com	Member	Global Administrator	Exchange Online (Plan 1)	50
Godzilla	godzilla@novacoastschool.com	Member	None	Microsoft 365 Business Premium	112
Hayley Marshall	hmarshall@novacoastschool.com	Member	None	None	1057
Henk Feenstra	hfeenstra@novacoastschool.com	Member	None	Microsoft 365 Business Premium	639
Hunter Arnell	-	Member	Global Administrator	None	1143

Name	Email	Type	Role	License	Days Since Last Login
Ian	-	Member	Global Administrator	None	1260
Janka Mihalik	jmihalik@novacoastschool.com	Member	None	Microsoft 365 Business Premium	689
Jared Pangretic	jpangretic@novacoastschool.com	Member	None	None	1121
Jennifer Evans	jjevans@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Jerry Smith	-	Member	None	None	1143
Joesph Valbert	jValbert@novacoastschool.com	Member	None	None	1129
Johnathan Cox	jcox@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Johnny Bananas	jbananas@M365EDU660802.onmicrosoft.com	Member	None	None	1144
Jolle Klos	jklos@novacoastschool.com	Member	None	Microsoft 365 Business Premium	954
Jordan Taj	jtaj@novacoastschool.com	Member	None	None	1129
Josh Rodriguez	jRodriguez@novacoastschool.com	Member	None	None	1108
jtaggart	-	Member	Global Administrator	None	1283
Kelechi Olelewe	KelechiOlelewe@novacoastschool.com	Member	Global Administrator	Microsoft Cloud App Security, Microsoft Power Automate Free, Microsoft 365 E5	316
Kenneth Crawford	kCrawford@novacoastschool.com	Member	None	None	1129
Klaus Dimmler	klaus@novacoastschool.com	Member	None	None	1205
Kyle Barthel	kbarthel@novacoastschool.com	Member	None	Microsoft 365 Business Premium	957
Kyle Menosky	kmenosky@novacoastschool.com	Member	None	Microsoft 365 Business Basic	660
Leroy Jenkins	-	Member	None	None	1143
Lisa Varilek	lvarilek@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807

Name	Email	Type	Role	License	Days Since Last Login
Luis Fagelson	lFagelson@novacoastschool.com	Member	None	None	1057
Manish	manish@novacoastschool.com	Member	Global Administrator	Microsoft 365 Business Premium	84
Marissa Guerrero	mguerrero@novacoastschool.com	Member	None	None	1152
Matt Huston	-	Member	Global Administrator	None	1128
Matt Zayas	-	Member	Global Administrator	Microsoft Power Automate Free	535
Matthew Davenport	mdavenport@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Mic Cohagan	mcohagan@novacoastschool.com	Member	None	Microsoft 365 Business Basic	478
Mitchell Lubbers	-	Member	Global Administrator	None	1341
Monica Lam He	mlamhe@novacoastschool.com	Member	None	Microsoft 365 Business Premium	931
Monica Lam He	monica@novacoastschool.com	Member	None	None	1054
Nate Brown	nBrown@novacoastschool.com	Member	None	None	1137
Nicholas Christians	nChristians@novacoastschool.com	Member	None	None	1129
Nick Conrad	nConrad@novacoastschool.com	Member	None	None	1129
Nick Ross	nross@novacoastschool.com	Member	None	Microsoft 365 Business Premium	442
Nick Ross	-	Member	None	None	1049
Nova Dev	dev@novacoastschool.com	Member	Global Administrator	None	1037
On-Premises Director	-	Member	Directory Synchronization Accounts	None	1049
Paul Torres	ptorres@novacoastschool.com	Member	None	Azure Active Directory Premium P1, Microsoft 365 E5	857
Peter Gerhardt	pgerhardt@novacoastschool.com	Member	None	Microsoft 365 Business Premium	694

Name	Email	Type	Role	License	Days Since Last Login
QA Admin	qa-admin@M365EDU660802.onmicrosoft.com	Member	Global Administrator	None	764
Robert Costin	rcostin@novacoastschool.com	Member	Global Administrator	None	388
Ryan Walsh	rwalsh@novacoastschool.com	Member	None	None	1242
Salman	-	Member	Global Administrator	None	135
Sara Feeny	sfeeny@novacoastschool.com	Member	None	Microsoft 365 Business Premium	673
Sheri Summers	SheriS@novacoastschool.com	Member	None	Microsoft Cloud App Security	1265
SSPR User021921	-	Member	None	Microsoft Power Automate Free	1134
Testing Forwards	testforward@novacoastschool.com	Member	None	None	1156
thetradingnest	thetradingnest@gmail.com	Guest	None	None	1138
Thomas Welton	twelton@novacoastschool.com	Member	None	None	1226
Tyler Stromberg	tstromberg@novacoastschool.com	Member	None	Exchange Online (Plan 1)	807
Walker Roe	wroe@novacoastschool.com	Member	None	None	1137
Wes Johnson	wesjohnson@novacoastschool.com	Member	Global Administrator	Microsoft 365 Business Premium	98
Young Fitzpatrick	YoungF@novacoastschool.com	Member	None	None	1265
Zachary Gibson	zgibson@novacoastschool.com	Member	None	None	1229

Global Admins

Name	Email	Type	Role	License	Days Since Last Login
Admin	admin@M365EDU660802.onmicrosoft.com	Member	Global Administrator	Microsoft Defender for Endpoint P2_XPLAT, Azure Active Directory Premium P1	104

Name	Email	Type	Role	License	Days Since Last Login
Alex Core	acore@novacoastschool.com	Member	Global Administrator	Microsoft 365 Business Premium	585
Austin Hampton	-	Member	Global Administrator	None	1137
Ebraheem	ebraheem@novacoastschool.com	Member	Global Administrator	Exchange Online (Plan 1)	1
Faisal	-	Member	Global Administrator	None	6
Girma-Selassie Tsega	gtsegay@novacoastschool.com	Member	Global Administrator	Exchange Online (Plan 1)	50
Global Admin	-	Member	Global Administrator	Microsoft Power Automate Free	-
Hunter Arnell	-	Member	Global Administrator	None	1143
Ian	-	Member	Global Administrator	None	1260
Joe Shuster	-	Member	Global Administrator	None	1
jtaggart	-	Member	Global Administrator	None	1283
Kelechi Olelewe	KelechiOlelewe@novacoastschool.com	Member	Global Administrator	Microsoft Cloud App Security, Microsoft Power Automate Free, Microsoft 365 E5	316
Manish	manish@novacoastschool.com	Member	Global Administrator	Microsoft 365 Business Premium	84
Matt Huston	-	Member	Global Administrator	None	1128
Matt Zayas	-	Member	Global Administrator	Microsoft Power Automate Free	535
Mike	-	Member	Global Administrator	None	-
Mitchell Lubbers	-	Member	Global Administrator	None	1341
MSPMagic Administrat	-	Member	Global Administrator	None	-
Nova Dev	dev@novacoastschool.com	Member	Global Administrator	None	1037

Name	Email	Type	Role	License	Days Since Last Login
QA Admin	qa-admin@M365EDU660802.onmicrosoft.com	Member	Global Administrator	None	764
Robert Costin	rcostin@novacoastschool.com	Member	Global Administrator	None	388
Salman	-	Member	Global Administrator	None	135
System Administrator	admin@novacoastschool.com	Member	Global Administrator	Microsoft Power Automate Free, Power Virtual Agents Viral Trial, Microsoft 365 Business Premium, Microsoft Defender for Identity	6
Waleed	-	Member	Global Administrator	None	-
Wes Johnson	wesjohnson@novacoastschool.com	Member	Global Administrator	Microsoft 365 Business Premium	98

Guest Users

Name	Email	Type	Role	License	Days Since Last Login
thetradingnest	thetradingnest@gmail.com	Guest	None	None	1138

Disabled Users with licenses

Name	Email	Type	Role	License	Days Since Last Login
Main Line in AT	-	Member	None	Microsoft Teams Phone Resource Account	-

Authentication Methods Policy

Evidence

ID	State	Number Matching Required
Fido2	disabled	N/A
MicrosoftAuthenticator	enabled	enabled
Sms	disabled	N/A

ID	State	Number Matching Required
TemporaryAccessPass	disabled	N/A
HardwareOath	disabled	N/A
SoftwareOath	disabled	N/A
Voice	disabled	N/A
Email	enabled	N/A
X509Certificate	disabled	N/A

User MFA Authentication Methods

The following users leverage only email and phone as their second factor. These are considered weaker forms of MFA. These users should leverage a strong MFA method like FIDO2 or Microsoft authenticator

User MFA Authentication Methods

User Name	Microsoft Authenticator	Phone	Email	Password	FIDO2	Windows Hello For Business	Temporary Access Pass	Software OAuth Token
Admin	true	true	true	true	false	false	false	false
Alex Wilber	false	true	true	true	false	false	false	false
Brigit Sviontek	false	false	true	true	false	false	false	false
Cara Coleman	false	true	false	true	false	false	false	false
Daisy Pike	false	false	true	true	false	false	false	false
Delbert McCray	true	true	true	true	false	false	false	false
Douglas Cothran	false	true	false	true	false	false	false	false
Eric Mink	false	false	true	true	false	false	false	false
Ethan Milner	true	true	false	true	false	false	false	false
Fatima Zapata	false	true	false	true	false	false	false	false
Geraldine Fricke	true	true	false	true	false	false	false	false
Girma-Selassie Tsega	false	false	true	true	false	false	false	false

User Name	Microsoft Authenticator	Phone	Email	Password	FIDO2	Windows Hello For Business	Temporary Access Pass	Software OAuth Token
Jolle Klos	false	false	true	true	false	false	false	false
Kelechi Olelewe	false	false	true	true	false	false	false	false
Kyle Barthel	true	true	false	true	false	false	false	false
Matt Huston	false	false	true	true	false	false	false	false
Matt Zayas	false	false	true	true	false	false	false	false
Mic Cohagan	true	true	false	true	false	false	false	false
Monica Lam He	false	false	true	true	false	false	false	false
Nick Conrad	false	false	true	true	false	false	false	false
Nova Dev	false	true	true	true	false	false	false	false
Ole Andersen	false	false	true	true	false	false	false	false
Paul Torres	false	false	true	true	false	false	false	false
Robert Costin	false	false	true	true	false	false	false	false
System Administrator	true	true	true	true	false	false	false	false
Wes Johnson	false	false	true	true	false	false	false	false

Groups

Summary

Total Groups	Distribution List	Groups with Disabled Users
60	1	0

Groups

Name	Type	Dynamic	Disabled Users in Group	Created Date	Members
Local Admin Test	Security	false	false	7/7/2022	3
Windows Autopatch Device Registration	Security	false	false	1/14/2023	0
Physical Science	Microsoft 365	false	false	4/3/2020	19

Name	Type	Dynamic	Disabled Users in Group	Created Date	Members
Retention	Microsoft 365	false	false	9/20/2022	1
Autopilot Devices	Security	true	false	12/21/2022	0
Venture Capital Research	Mail-Enabled Security	false	false	4/3/2020	16
Modern Workplace Devices-Windows Autopatch-Fast	Security	false	false	1/14/2023	0
Security Group 1	Security	false	false	7/27/2020	19
Datto Test	Microsoft 365	false	false	10/21/2023	19
Sharepoint 2	Microsoft 365	false	false	7/27/2020	16
Test Device	Security	true	false	12/21/2022	0
macOS Deployment	Security	false	false	8/22/2020	9
Azure ATP m365edu660802 Users	Security	false	false	9/3/2021	0
Modern Workplace Roles - Service Reader	Security	false	false	1/14/2023	0
Pineview School Science Teachers	Microsoft 365	false	false	4/3/2020	8
Share point 3	Microsoft 365	false	false	7/27/2020	6
Modern Workplace Roles - Service Administrator	Security	false	false	1/14/2023	0
Windows Autopatch - Ring1	Security	false	false	1/14/2023	0
Azure ATP m365edu660802 Administrators	Security	false	false	9/3/2021	0
Pineview School District Principals	Microsoft 365	false	false	4/3/2020	2
SSPR	Security	false	false	2/9/2021	2
Windows Autopatch - Ring3	Security	false	false	1/14/2023	0
Deployment team	Microsoft 365	false	false	8/31/2021	5
Distribution Test	Distribution List	false	false	11/5/2021	0
Pineview School Staff	Microsoft 365	false	false	4/3/2020	9
Share point 4	Microsoft 365	false	false	7/27/2020	3
Azure ATP m365edu660802 Viewers	Security	false	false	9/3/2021	0
Local Admin Group	Security	false	false	12/16/2022	1
Windows Autopatch - Last	Security	false	false	1/14/2023	0

Name	Type	Dynamic	Disabled Users in Group	Created Date	Members
Modern Workplace-All	Security	false	false	1/14/2023	0
Modern Workplace Devices-Windows Autopatch-First	Security	false	false	1/14/2023	0
All Users	Security	true	false	6/16/2020	20
B20S Entrepreneurship Course	Microsoft 365	false	false	4/3/2020	12
TEST site	Microsoft 365	false	false	8/16/2022	1
Windows Autopatch - Devices All	Security	false	false	12/11/2023	0
Win10Devicesv2	Security	true	false	5/25/2021	10
Test Intune deployment	Security	false	false	3/8/2021	0
Exchange Admin Group	Security	false	false	12/20/2022	1
Operations group	Microsoft 365	false	false	2/15/2021	3
All Company	Microsoft 365	false	false	7/25/2020	7
Office Group	Mail-Enabled Security	false	false	7/27/2020	4
Health Research	Microsoft 365	false	false	4/3/2020	19
AAD DC Administrators	Security	false	false	1/27/2023	0
Mail-Enabled Test	Mail-Enabled Security	false	false	11/5/2021	0
Windows Autopatch - Ring2	Security	false	false	1/14/2023	0
Modern Workplace Devices-All	Security	false	false	1/14/2023	0
TestDynamic	Mail-Enabled Security	true	false	11/5/2021	1
Algebra	Microsoft 365	false	false	4/3/2020	19
Novacoast School of Mines	Microsoft 365	false	false	1/14/2021	20
Modern Workplace Devices-Windows Autopatch-Broad	Security	false	false	1/14/2023	0
PurviewComplianceTst-ko	Security	false	false	1/27/2023	0
Modern Workplace Devices-Virtual Machine	Security	false	false	1/14/2023	0
My Sharepoint Site1	Microsoft 365	false	false	7/27/2020	1
MSFTD4E_Test_KO	Security	false	false	5/14/2021	0

Name	Type	Dynamic	Disabled Users in Group	Created Date	Members
Batcave	Mail-Enabled Security	false	false	2/5/2023	1
Win10Devices	Security	true	false	5/25/2021	10
Modern Workplace Devices-Windows Autopatch-Test	Security	false	false	1/14/2023	0
MZ test group	Mail-Enabled Security	false	false	8/27/2021	0
Excelsior Team	Microsoft 365	false	false	2/5/2021	3
Windows Autopatch - Test	Security	false	false	1/14/2023	0
Test Team	Microsoft 365	false	false	4/5/2021	20

Enterprise Applications

Summary

Total Enterprise Apps	SSO Enabled Apps
26	1

Enterprise Apps

Name	SSO Enabled	Created Date
dxprovisioning-worker-mfa	false	4/3/2020
MOD Demo Platform UnifiedApiConsumer	false	4/3/2020
dxprovisioning-analytics	false	7/24/2020
Microsoft Intune PowerShell	false	8/22/2020
ManageEngine M365 Security Plus v1	false	8/25/2020
Pax8 Pro Consent (Dev)	false	4/16/2020
Dropbox Business	true	10/24/2020
Microsoft Cloud App Security (Internal)	false	10/25/2020
SkyKick Cloud Manager	false	11/1/2020
Salesforce	false	11/7/2020
Pax8 Pro Consent	false	10/29/2020
Cloud Assessment (Dev)	false	11/30/2020

Name	SSO Enabled	Created Date
Graph Explorer	false	2/16/2021
Cloud Assessment	false	3/4/2021
Pax8 Pro Graph	false	3/8/2021
Pax8 Pro Consent	false	3/15/2021
Pax8 to Customer	false	5/18/2021
MCAT	false	6/8/2021
Voleer Template Automation	false	9/16/2021
MTM	false	11/22/2020
NCE Tracker	false	1/7/2022
Modern Workplace Tools	false	12/17/2020
Pax8Preproduction	false	12/7/2022
Simeon Cloud Installer	false	1/31/2023
Overe Ltd.	false	11/23/2023
Cloud Capsule	false	3/24/2024

Conditional Access Policies

Summary

Total Conditional Access Policies	Users being excluded from MFA enforced Policies
10	4

Conditional Access Policy

Name	State	Users	Apps/Actions	Conditions	Block/ Grant Access	Session Controls
MCAS Test	On	• Users included: 1 specific user, 1 specific role • Users excluded: None	• Policy applies to: apps • Apps included: 2 specific apps • Apps excluded: None	• Device platforms included: all • Device platforms excluded: android, iOS, macOS, linux • Client apps included: browser, mobileAppsAndDesktopClients	Allow access but require mfa	None

Name	State	Users	Apps/Actions	Conditions	Block/ Grant Access	Session Controls
CA Test	On	• Users included: 1 specific user • Users excluded: 20 specific users	• Policy applies to: apps • Apps included: All • Apps excluded: None	• Client apps included: all	Allow access but require mfa	None
Intune Enrollment Exception	Off	• Users included: All • Users excluded: None	• Policy applies to: apps • Apps included: 1 specific app • Apps excluded: None	• Locations included: All • Client apps included: all	Allow access but require mfa	None
Lighthouse Test	On	• Users included: 19 specific users • Users excluded: None	• Policy applies to: apps • Apps included: All • Apps excluded: None	• Client apps included: all	Allow access but require mfa	None
Device Compliance	On	• Users included: 2 specific users • Users excluded: None	• Policy applies to: apps • Apps included: All • Apps excluded: None	• Client apps included: all	Allow access but require Phishing-resistant MFA	None
Disable Basic Auth	On	• Users included: All • Users excluded: 1 specific user	• Policy applies to: apps • Apps included: All • Apps excluded: None	• Client apps included: exchangeActiveSync, other	Block	None
Require Device Compliance	On	• Users included: All • Users excluded: 1 specific user	• Policy applies to: apps • Apps included: All • Apps excluded: None	• Device platforms included: all • Device platforms excluded: android, iOS, macOS, linux • Client apps included: all	Allow access but require compliant Device, or domainJoinedDevice	None
Block High Risk Users	On	• Users included: All • Users excluded: 1 specific user	• Policy applies to: apps • Apps included: None • Apps excluded: None	• Client apps included: all	Block	None
Require approved client apps or app protection policies	On	• Users included: All • Users excluded: 1 specific user	• Policy applies to: apps • Apps included: All • Apps excluded: None	• Device platforms included: android, iOS • Client apps included: all	Allow access but require approvedApplication, or compliant Application	None

Name	State	Users	Apps/Actions	Conditions	Block/ Grant Access	Session Controls
Microsoft-managed: Multifactor authentication for admins accessing Microsoft Admin Portals	On	• Users included: 14 specific roles • Users excluded: None	• Policy applies to: apps • Apps included: 1 specific app • Apps excluded: None	• Client apps included: all	Allow access but require mfa	None

Licensed users excluded from CA that enforces MFA

Name	Conditional Access policy
CA Test	Ebraheem, System Administrator, Alex Wilber, Admin

Sign Ins

The following are considered riskier sign ins due to factors such as Conditional Access not being applied, noncompliant devices signing in, and more.

Sign Ins

User	Date	IP Address	Location	Application	Risk	Request ID
Ebraheem	3/23/2024	103.157.88.21	Attock, Punjab	Cloud Capsule	Conditional Access Not Applied	96f9611a-376d-4271-b14b-63ec82545900
f2e51bfb-d8dd-4645-aa25-6990cc3cfff8	3/30/2024	24.120.54.100	,	OfficeHome	Conditional Access Not Applied	cc5175d7-8ee9-4fd9-a80b-7e8b7a5f2600
System Administrator	3/30/2024	24.120.54.100	Las Vegas, Nevada	Cloud Capsule	Conditional Access Not Applied	f9864900-3884-45c9-b5fa-05f1e6f03700
System Administrator	3/30/2024	24.120.54.100	Las Vegas, Nevada	Cloud Capsule	Conditional Access Not Applied	0cf3df3a-4e7f-4ec6-9149-04fb582c3e00
Ebraheem	3/30/2024	2407:d000:1a:9251:c025:eff2:2740:60ca	,	Graph Explorer	Conditional Access Not Applied	1be7898e-9837-4b8b-a123-1aca64696600
Ebraheem	3/29/2024	2407:d000:1a:7d0b:e9f4:8f7d:c29e:c13c	,	Cloud Capsule	Conditional Access Not Applied	a62907d2-3a0b-4b79-a48c-0a95cf7b7500

User	Date	IP Address	Location	Application	Risk	Request ID
Ebraheem	3/29/2024	2407:d000:1a:7d0b:2df7:a5e4:28d3:c9cf	,	Graph Explorer	Conditional Access Not Applied	d585dd52-7711-4d7d-8e63-ff6efd7f1b00
Ebraheem	3/29/2024	2407:d000:1a:7d0b:2df7:a5e4:28d3:c9cf	,	Graph Explorer	Conditional Access Not Applied	112cb76a-0b5c-411e-a25f-cb74f1772300
Ebraheem	3/29/2024	2407:d000:1a:7d0b:e9f4:8f7d:c29e:c13c	,	Cloud Capsule	Conditional Access Not Applied	f5451ee7-1b4d-427a-a6c0-14c3ed5d1f00
Joe Shuster	3/28/2024	2601:280:c600:4d00:c8:7d0:dce8:33ed	Aurora, Colorado	Azure Portal	Conditional Access Not Applied	3e05ed05-531f-495d-8c71-1a805bae6301

Risk Detections

User	Risk State	Risk Level	IP Address	Location	Detected Time	Last Update Time	Risk Event Type
System Administrator	At Risk	Medium	2600:100e:b083:c456::	Ashburn, Virginia	1/30/2024	1/30/2024	anomalousToken
Ebraheem	At Risk	Low	115.186.57.250	Lahore, Punjab	3/20/2024	3/20/2024	unfamiliarFeatures
Ebraheem	At Risk	Low	103.157.88.21	Attock, Punjab	3/23/2024	3/23/2024	unfamiliarFeatures
Ebraheem	At Risk	Low	115.186.57.250	Lahore, Punjab	3/20/2024	3/20/2024	unfamiliarFeatures

Domains

Summary

Total Domains	Unhealthy Domains
2	2

Domains

Domain Name	Is Default	Is Verified	DNS Provider	MX Record	SPF Check	DMARC Check	DKIM Enabled
asdf.com	false	false	DreamHost	mx10.asdf.com	Fail	Fail	

Domain Name	Is Default	Is Verified	DNS Provider	MX Record	SPF Check	DMARC Check	DKIM Enabled
M365EDU660802.onmicrosoft.com	false	true	Microsoft Corporation	M365EDU660802.mail.protection.outlook.com	Pass	Fail	
novacoastschool.com	true	true			Fail	Fail	
M365EDU660802.mail.onmicrosoft.com	false	true	Microsoft Corporation	m365edu660802-mail-onmicrosoft-com.mail.protection.outlook.com, m365edu660802-mail-onmicrosoft-com.mail.protection.outlook.com	Pass	Fail	

Devices

Summary

Total Enabled Devices	Stale Devices
10	10

Personal Devices not enrolled in MDM

Device	User	Enabled	Ownership	Device Type	Registration Date	Last Sign In	Enrollment Type	MDM Controlled	OS
No Record Found									

Stale Devices

Device	User	Enabled	Ownership	Device Type	Registration Date	Last Sign In	Enrollment Type	MDM Controlled	OS
ITV7	Arden Asher	true	Company	RegisteredDevice	5/22/2021	5/22/2021	Hybrid Azure AD joined	true	Windows
DESKTOP-N9J8THC	Kelechi Olelewe	true	Company	RegisteredDevice	5/14/2021	6/3/2021	Azure AD Joined	false	Windows
ALEXW-PC	Alex Wilber	true	Personal	RegisteredDevice	4/1/2023	4/1/2023	Azure AD Registered	true	Windows
ITV6	Kyle Barthel	true	Company	RegisteredDevice	5/16/2021	6/1/2021	Hybrid Azure AD joined	false	Windows

Device	User	Enabled	Ownership	Device Type	Registration Date	Last Sign In	Enrollment Type	MDM Controlled	OS
ITV5	Kyle Barthel	true	Company	RegisteredDevice	7/28/2021	10/8/2021	Hybrid Azure AD joined	true	Windows
IntuneTestV5	Nick Ross	true	Company	RegisteredDevice	5/16/2021	5/16/2021	Hybrid Azure AD joined	false	Windows
ITV8	Arden Asher	true	Company	RegisteredDevice	5/22/2021	7/28/2021	Hybrid Azure AD joined	false	Windows
WINDEV2311EVAL	Godzilla	true	Personal	RegisteredDevice	12/8/2023	12/8/2023	Azure AD Registered	true	Windows
ITV4	Kyle Barthel	true	Company	RegisteredDevice	7/28/2021	8/15/2021	Hybrid Azure AD joined	false	Windows
ITV9	Kyle Barthel	true	Company	RegisteredDevice	5/22/2021	5/22/2021	Hybrid Azure AD joined	false	Windows

Intune

Summary

Noncompliant Devices	Devices without Encryption	Devices with 90%+ Storage	Devices with Active Malware
2	2	0	0

Noncompliant Devices

Device	User	Compliant	OS	Autopilot Device	Encrypted	Type	Last Sync Date	Active Malware	Storage Used
ALEXW-PC	Alex Wilber	false	Windows 10.0.22621.1413	false	false	personal	4/1/2023	0	26GB/126GB
WINDEV2311EVAL	Godzilla	false	Windows 10.0.22621.2715	false	false	personal	12/8/2023	0	52GB/124GB

Devices without encryption

Device	User	Compliant	OS	Autopilot Device	Encrypted	Type	Last Sync Date	Active Malware	Storage Used
ALEXW-PC	Alex Wilber	false	Windows 10.0.22621.1413	false	false	personal	4/1/2023	0	26GB/126GB
WINDEV2311EVAL	Godzilla	false	Windows 10.0.22621.2715	false	false	personal	12/8/2023	0	52GB/124GB

Devices with Active malware

Device	User	Compliant	OS	Autopilot Device	Encrypted	Type	Last Sync Date	Active Malware	Storage Used

Device	User	Compliant	OS	Autopilot Device	Encrypted	Type	Last Sync Date	Active Malware	Storage Used
No Record Found									

Devices with 90% storage

Device	User	Compliant	OS	Autopilot Device	Encrypted	Type	Last Sync Date	Active Malware	Storage Used
No Record Found									

App Protection Policies

App Protection Policies

Policy Name	Policy Type	Created Date	Assigned
iOS_APP_PROTECT	iOS	Sun Feb 05 2023	true
iOS Default	iOS	Sun Feb 05 2023	false
Android App Protection	Android	Thu Nov 11 2021	true

Compliance Policies

Summary

Policies with Non Compliant Devices
0

Compliance Policies

Policy Name	Platform	Compliant Devices	Non Compliant Devices	Created Date	Last Updated
Default compliance policy for Android	android	0	0	6/16/2020	6/16/2020
iOS Compliance	ios	0	0	11/11/2021	11/11/2021
macOS Compliance	macOS	0	0	11/11/2021	11/11/2021
Test	windows10	0	0	5/16/2021	5/16/2021

Intune Applications

Summary

Total Apps	Apps with Failures
12	0

Intune Applications

App Name	App Type	Assigned	App Install Status	Created Date	Last Updated
Abobe	Windows app (Win32)	No	• Installed: 0 • Failed: 0	2/13/2023	2/13/2023
Adobe Creative Cloud	Microsoft Store app	Yes	• Installed: 0 • Failed: 0	1/12/2023	1/12/2023
Adobe Fresco	Microsoft Store app	No	• Installed: 0 • Failed: 0	10/26/2023	10/26/2023
Box	Android Store App	Yes	• Installed: 0 • Failed: 0	11/12/2021	11/12/2021
GoolgeChrome	Windows app (Win32)	No	• Installed: 0 • Failed: 0	2/13/2023	2/13/2023
Microsoft 365 Apps for Windows 10	Microsoft 365 Apps	Yes	• Installed: 2 • Failed: 0	8/16/2021	8/16/2021
Microsoft 365 Apps for Windows 10 and later	Microsoft 365 Apps	No	• Installed: 0 • Failed: 0	11/16/2023	11/16/2023
Microsoft Authenticator	iOS Store App	Yes	• Installed: 0 • Failed: 0	11/12/2021	11/12/2021
Microsoft Intune Company Portal	iOS Store App	No	• Installed: 0 • Failed: 0	2/5/2023	2/5/2023
Test Web Link	Windows Web Link	No	• Installed: 0 • Failed: 0	10/26/2023	10/26/2023
TikTok	iOS Store App	Yes	• Installed: 0 • Failed: 0	4/14/2023	4/14/2023
Yubico Authenticator	Windows Line of Business App	No	• Installed: 0 • Failed: 0	10/26/2023	10/26/2023

Configuration Profiles

Summary

Profiles with Assignment Failures
1

Configuration Profiles

Policy Name	Description	OS	Assigned	Policy Type	Created Date	Last Updated	Assignment Status
AddLocalAdmin		Windows	Yes	Custom	12/16/2022	12/16/2022	• 0 Devices Successful • 0 Failures
ASR Rules		windows10	Yes	endpointSecurityAttackSurfaceReduction	8/19/2023	8/19/2023	• 0 Devices Successful • 0 Failures
Augustine Test	Augustine Test	windows10	Yes	endpointSecurityEndpointDetectionAndResponse	12/5/2023	12/5/2023	• 0 Devices Successful • 0 Failures
Bitlocker Test		Windows	No	Endpoint Protection	10/26/2023	10/26/2023	• 0 Devices Successful • 0 Failures
Bitlocker-Security Test		windows10	No	endpointSecurityDiskEncryption	10/26/2023	10/26/2023	• 0 Devices Successful • 0 Failures
Creating Local Admin		Windows	Yes	Custom	12/15/2022	12/15/2022	• 0 Devices Successful • 1 Failures
Default iOS device policy for EDU	Default iOS device policy for Intune for Education	iOS	Yes	iosGeneralDeviceConfiguration	4/3/2020	4/3/2020	• 0 Devices Successful • 0 Failures
Intune data collection policy	Windows Health Monitoring policy for Endpoint Analytics	Windows	Yes	Health Monitoring	1/14/2023	1/14/2023	• 0 Devices Successful • 0 Failures
macOS MDATP Full Disk Access		macOS	Yes	macOSCustomConfiguration	8/25/2020	8/25/2020	• 0 Devices Successful • 0 Failures
macOS MDATP Full Disk Access		macOS	Yes	macOSCustomConfiguration	8/23/2020	8/23/2020	• 0 Devices Successful • 0 Failures
macOS MDATP Kernel Extension		macOS	Yes	macOSCustomConfiguration	8/23/2020	8/23/2020	• 0 Devices Successful • 0 Failures
macOS MDATP Kernel Extension		macOS	Yes	macOSCustomConfiguration	8/25/2020	8/25/2020	• 0 Devices Successful • 0 Failures
macOS MDATP Notifications		macOS	Yes	macOSCustomConfiguration	8/25/2020	8/25/2020	• 0 Devices Successful • 0 Failures

Policy Name	Description	OS	Assigned	Policy Type	Created Date	Last Updated	Assignment Status
macOS MDATP Notifications		macOS	Yes	macOSCustomConfiguration	8/23/2020	8/23/2020	• 0 Devices Successful • 0 Failures
macOS MDATP Onboarding		macOS	Yes	macOSCustomConfiguration	8/23/2020	8/23/2020	• 0 Devices Successful • 0 Failures
macOS MDATP Onboarding		macOS	Yes	macOSCustomConfiguration	8/25/2020	8/25/2020	• 0 Devices Successful • 0 Failures
MacOS Update Profile		macOS	No	macOSSoftwareUpdateConfiguration	11/11/2023	11/11/2023	• 0 Devices Successful • 0 Failures
OneDrive_Silent_Move		Windows	Yes	Administrative Template	8/17/2021	8/17/2021	• 1 Devices Successful • 0 Failures
OneDrive_Silent_Move		Windows	Yes	Administrative Template	8/16/2021	8/16/2021	• 2 Devices Successful • 0 Failures
Pilot Profile		windows10	Yes	endpointSecurityEndpointPrivilegeManagement	4/1/2023	4/1/2023	• 0 Devices Successful • 0 Failures
Test	TEst	Windows	Yes	windows10GeneralConfiguration	7/28/2021	7/28/2021	• 2 Devices Successful • 0 Failures
Test Profile		windows10	Yes	endpointSecurityAntivirus	6/13/2023	6/13/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - Data Collection	Allows diagnostic data from this device to be processed by Windows Autopatch. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	7/25/2023	• 0 Devices Successful • 0 Failures

Policy Name	Description	OS	Assigned	Policy Type	Created Date	Last Updated	Assignment Status
Windows Autopatch - Edge Update Channel Beta	Deploys Edge Beta Channel Updates. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	1/14/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - Edge Update Channel Stable	Deploys Edge Stable Channel Updates. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	1/14/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - MDM wins over GPO	Sets MDM to win over GPO. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	1/14/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - Office Configuration	Sets Office Update Channel to the Monthly Enterprise servicing branch. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	3/5/2024	• 0 Devices Successful • 0 Failures

Policy Name	Description	OS	Assigned	Policy Type	Created Date	Last Updated	Assignment Status
Windows Autopatch - Office Update Configuration - Expedited	Expedited updates for CVE-2023-23397	windows10	Yes	Setting Catalog	3/16/2023	3/16/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - Office Update Configuration [Broad]	Sets Office Update Deadline. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	No	Setting Catalog	6/13/2023	6/13/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - Office Update Configuration [Fast]	Sets Office Update Deadline. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	No	Setting Catalog	6/5/2023	11/13/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch - Office Update Configuration [First]	Sets Office Update Deadline. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	3/30/2023	• 0 Devices Successful • 0 Failures

Policy Name	Description	OS	Assigned	Policy Type	Created Date	Last Updated	Assignment Status
Windows Autopatch - Office Update Configuration [Test]	Sets Office Update Deadline. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will overwrite any changes.	windows10	Yes	Setting Catalog	1/14/2023	3/29/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch Update Policy - Default - Last	Created by system	Windows	Yes	Update Configuration	7/25/2023	7/25/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch Update Policy - Default - Ring1	Windows Update for Business Configuration for the First Ring	Windows	Yes	Update Configuration	1/14/2023	8/5/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch Update Policy - Default - Ring2	Windows Update for Business Configuration for the Fast Ring	Windows	Yes	Update Configuration	1/14/2023	8/5/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch Update Policy - Default - Ring3	Windows Update for Business Configuration for the Broad Ring	Windows	Yes	Update Configuration	1/14/2023	8/5/2023	• 0 Devices Successful • 0 Failures
Windows Autopatch Update Policy - Default - Test	Windows Update for Business Configuration for the Test Ring	Windows	Yes	Update Configuration	1/14/2023	8/5/2023	• 0 Devices Successful • 0 Failures
Windows Update policy	Windows Update policy	Windows	No	Update Configuration	4/3/2020	4/3/2020	• 0 Devices Successful • 0 Failures

Teams

Summary

Total Teams
14

Teams

Name	Standard Channels	Private Channels	Shared Channels	Team Members	Owners	Guests	Privacy
Algebra	5	0	0	19	3	0	hiddenMembership
B20S Entrepreneurship Course	4	0	0	12	6	0	hiddenMembership
Batcave	0	0	0	0	0	0	public
Datto Test	1	0	0	30	1	0	public
Deployment team	2	0	0	5	1	0	private
Excelsior Team	1	0	0	3	1	0	private
Health Research	4	0	0	30	3	0	public
Novacoast School of Mines	1	0	0	223	28	0	public
Physical Science	5	0	0	26	4	0	hiddenMembership
Pineview School District Principals	1	0	0	2	1	0	private
Pineview School Science Teachers	4	0	0	8	5	0	private
Pineview School Staff	6	0	0	9	1	0	private
Test Team	2	0	0	222	27	0	public
Venture Capital Research	5	0	0	16	4	0	private

Teams Activities

Summary

Total Users 30+ Days inactive
5

Users with 30+ days of inactivity

Name	Last Active Date	Chat Count	Call Count	Meeting Count	Days Since Last Activity
acore@novacoastschool.com	6/29/2022	0	0	0	640
admin@novacoastschool.com	2/18/2024	0	0	0	41

Name	Last Active Date	Chat Count	Call Count	Meeting Count	Days Since Last Activity
AlexW@novacoastschool.com	4/1/2023	0	0	0	364
kbarthel@novacoastschool.com	6/1/2021	0	0	0	1033
mzayas@novacoastschool.com	11/2/2021	0	0	0	879

Teams Application Settings

Policy Name	Microsoft Apps	Third-Party Apps	Custom Apps
Global	Allow All Apps	App Restrictions	Allow All Apps

Teams External Access Policy

Policy Name	External Domain Access	External Chats to Unmanaged users	Inbound Chats from Unmanaged users	Communication with Skype users
Global	Block all external domains	true	false	false

Teams File Sharing Settings

Policy Name	Allow Dropbox	Allow Box	Allow Google Drive	Allow Citrix Files	Allow Egnyte
Global	true	true	true	false	true

Teams Meeting Policies

Policy Name	Allow External Participants to Request Control	Allow Anonymous Users to Start Meetings	Allow Automatic Meeting Admittance to Anonymous users	Meeting Recording Default Expiration Time
Global	false	false	true	120
Tag:AllOn	false	false	true	120
Tag:RestrictedAnonymousAccess	false	false	true	120
Tag:AllOff	false	false	true	120

Policy Name	Allow External Participants to Request Control	Allow Anonymous Users to Start Meetings	Allow Automatic Meeting Admittance to Anonymous users	Meeting Recording Default Expiration Time
Tag:RestrictedAnonymousNoRecording	false	false	true	120
Tag:Default	false	false	true	120
Tag:Kiosk	false	false	true	120

Exchange

Mailboxes

Summary

Mailboxes over 90% storage	Shared Mailboxes with License
0	1

Mailboxes over 90% storage

Name	Type	Storage Used	Storage Avaiable	Last Activity date	Has Archive	Is Licensed	Is Shared
No Record Found							

Shared Mailboxes with a license

Name	Type	Storage Used	Storage Avaiable	Last Activity date	Has Archive	Is Licensed	Is Shared
Bruce Wayne	Shared	0GB	50GB	8/15/2022	false	true	true

Inactive Mailboxes

Name	Type	Storage Used	Storage Avaiable	Last Activity date	Has Archive	Is Licensed	Is Shared
System Administrator	User	0GB	50GB	2/27/2024	false	true	false
Alex Wilber	User	0GB	50GB	5/14/2023	false	true	false
Alex Core	User	0GB	50GB	5/4/2021	true	true	false
Girma-Selassie Tsegay	User	0GB	50GB	2/8/2024	true	true	false
Kelechi Olelewe	User	0GB	100GB	3/24/2023	false	true	false
Daisy Pike	User	0GB	50GB	8/24/2021	false	true	false
Darryn McGuire	User	0GB	50GB	1/20/2022	false	true	false
Dylan Feske	User	0GB	50GB	1/12/2022	false	true	false

Name	Type	Storage Used	Storage Avaiable	Last Activity date	Has Archive	Is Licensed	Is Shared
Paul Torres	User	0GB	100GB	6/24/2021	false	true	false
Johnathan Cox	User	0GB	50GB	1/12/2022	false	true	false
Lisa Varilek	User	0GB	50GB	1/12/2022	false	true	false
Monica Lam He	User	0GB	50GB	9/10/2021	false	true	false
Matthew Davenport	User	0GB	50GB	1/12/2022	false	true	false
Janka Mihalik	User	0GB	50GB	4/26/2022	false	true	false
Brigit Sviontek	User	0GB	50GB	8/26/2021	false	true	false
Cliff Graham	User	0GB	50GB	1/12/2022	false	true	false

SharePoint

Summary

Total SharePoint Sites
31

Share Points Sites

Site Name	Short Name	Site URL	Created Date	Last Updated
CP	CP	https://m365edu660802.sharepoint.com/sites/CP	11/20/2023	11/20/2023
Datto Test	DattoTest	https://m365edu660802.sharepoint.com/sites/DattoTest	10/21/2023	10/8/2023
Batcave	Batcave959	https://m365edu660802.sharepoint.com/sites/Batcave959	2/5/2023	2/5/2023
Retention	retention	https://m365edu660802.sharepoint.com/sites/retention	9/20/2022	9/11/2022
TEST site	TESTsite	https://m365edu660802.sharepoint.com/sites/TESTsite	8/16/2022	7/31/2022
TestDynamic	TestDynamic	https://m365edu660802.sharepoint.com/sites/TestDynamic	11/5/2021	10/24/2021
Deployment team	DeploymentTeam	https://m365edu660802.sharepoint.com/sites/DeploymentTeam	8/31/2021	8/22/2021
MZ test group	MZtestgroup	https://m365edu660802.sharepoint.com/sites/MZtestgroup	8/27/2021	8/22/2021
Test Team	TestTeam	https://m365edu660802.sharepoint.com/sites/TestTeam	4/5/2021	4/4/2021
Operations group	operations2019	https://m365edu660802.sharepoint.com/sites/operations2019	2/15/2021	2/14/2021
Excelsior Team	ExcelsiorTeam	https://m365edu660802.sharepoint.com/sites/ExcelsiorTeam	2/5/2021	1/24/2021

Site Name	Short Name	Site URL	Created Date	Last Updated
Novacoast School of Mines	NovacoastSchoolofMines	https://m365edu660802.sharepoint.com/sites/NovacoastSchoolofMines	1/14/2021	1/10/2021
My Sharepointsite	MySharepointsite	https://m365edu660802.sharepoint.com/sites/MySharepointsite	7/27/2020	7/19/2020
Share point 3	Sharepoint3	https://m365edu660802.sharepoint.com/sites/Sharepoint3	7/27/2020	7/19/2020
Sharepoint 2	sp2	https://m365edu660802.sharepoint.com/sites/sp2	7/27/2020	7/19/2020
Share point 4	Sharepoint4	https://m365edu660802.sharepoint.com/sites/Sharepoint4	7/27/2020	7/19/2020
All Company	allcompany	https://m365edu660802.sharepoint.com/sites/allcompany	7/25/2020	7/19/2020
Office Group	OfficeGroup	https://m365edu660802.sharepoint.com/sites/OfficeGroup	7/27/2020	7/19/2020
My Sharepoint Site1	MySharepointSite1	https://m365edu660802.sharepoint.com/sites/MySharepointSite1	7/27/2020	7/19/2020
Team Site	contentTypeHub	https://m365edu660802.sharepoint.com/sites/contentTypeHub	4/3/2020	4/3/2020
Communication site	m365edu660802.sharepoint.com	https://m365edu660802.sharepoint.com	4/3/2020	3/29/2020
Pineview School Science Teachers	PineviewSchoolScienceTeachers	https://m365edu660802.sharepoint.com/sites/PineviewSchoolScienceTeachers	4/3/2020	3/29/2020
Algebra	Algebra	https://m365edu660802.sharepoint.com/sites/Algebra	4/3/2020	3/29/2020
Pineview School Staff	PineviewSchoolStaff	https://m365edu660802.sharepoint.com/sites/PineviewSchoolStaff	4/3/2020	3/29/2020
Health Research	HealthResearch	https://m365edu660802.sharepoint.com/sites/HealthResearch	4/3/2020	3/29/2020
B20S Entrepreneurship Course	B20SEntrepreneurshipCourse	https://m365edu660802.sharepoint.com/sites/B20SEntrepreneurshipCourse	4/3/2020	3/29/2020
Physical Science	PhysicalScience	https://m365edu660802.sharepoint.com/sites/PhysicalScience	4/3/2020	3/29/2020
Venture Capital Research	VentureCapitalResearch	https://m365edu660802.sharepoint.com/sites/VentureCapitalResearch	4/3/2020	3/29/2020

Site Name	Short Name	Site URL	Created Date	Last Updated
Pineview School District Principals	PineviewSchoolDistrictPrincipals	https://m365edu660802.sharepoint.com/sites/PineviewSchoolDistrictPrincipals	4/3/2020	3/29/2020
Community	Community	https://m365edu660802.sharepoint.com/portals/Community	4/3/2020	1/1/1
PointPublishing Hub Site	hub	https://m365edu660802.sharepoint.com/portals/hub	4/3/2020	1/1/1

SharePoint Settings

Sharing Policy	Limit External Sharing by Domain	Allowed domain list	Legacy Auth Enabled	Allow Guest to Share Items they don't own	Guest must sign in using the same account to which sharing invitations are sent
Anyone	true	• tminus365.com	No	Yes	Yes

OneDrive

OneDrive Stats

Summary

Users without Activity	OneDrive over 90% capacity
4	0

OneDrive Storage over 90% capacity

User	Storage Used	File Count	Last Activity Date
No Record Found			

OneDrive without activity

User	Storage Used	File Count	Last Activity Date
Matt Zayas	0GB/1024GB	1	4/5/2021
Kelechi Olelewe	0GB/1024GB	1	1/27/2023
Alex Wilber	0GB/1024GB	4	8/23/2020

Defender

Secure Score

Secure Score	Points Achieved
51.67%	434/840

Defender Devices

Device Name	Last Seen	OsPlatform	RiskScore	ExposureLevel
windev2311eval	Thu Dec 07 2023	Windows11	Low	Medium
windev2311eval	Fri Dec 08 2023	Windows11	Low	Medium