ACCESS CONTROL POLICY

Version 1.0

Updated By: Bradley Harrison

On the Date: 14th April 2023

Stackle

Table of Contents

1. Introduction

The Access Control Policy for Stackle serves as a comprehensive framework for managing access to the organization's information assets and systems, ensuring the right balance between security and usability. The policy is designed to protect Stackle's data and IT resources from unauthorized access and potential security incidents while providing authorized users with the appropriate level of access required to perform their job functions effectively.

Key aspects of the policy include:

1.1. Role-Based Access Control (RBAC): Access rights are granted based on predefined roles that align with users' job responsibilities, ensuring that users have the minimum necessary access to perform their tasks.

1.2. User Access Requests: A formal process is in place for requesting, authorizing, and granting access rights. This process includes approval by the user's manager and the IT department, ensuring that access rights are assigned appropriately.

1.3. Authentication: Users are required to authenticate themselves using unique credentials before accessing Stackle's information assets and systems. Strong password requirements and multi-factor authentication help secure user accounts.

1.4. Access Review and Monitoring: Periodic reviews of user access rights and monitoring of access logs help identify and address potential security risks, policy violations, or unnecessary access rights.

1.5. Access Termination: When an employee leaves the company or changes job roles, their access rights are promptly revoked or modified to prevent unauthorized access to information assets and systems.

1.6. Third-Party Access: Access rights for contractors and third parties are strictly controlled and limited to the minimum necessary to perform their contracted services. These external users must comply with Stackle's security policies and sign Non-Disclosure Agreements (NDAs) when handling sensitive information.

2. Purpose

The purpose of this Access Control Policy is to define and implement a structured and consistent approach to granting, managing, and revoking access to Stackle's information assets and systems. By establishing clear rules and guidelines, this policy seeks to balance the need for secure and controlled access with the operational requirements of the organization.

One of the primary objectives of this policy is to protect the confidentiality of Stackle's sensitive and proprietary information. This is achieved by ensuring that access is granted only to individuals who have a legitimate need to access the information based on their job responsibilities, and by preventing unauthorized access and potential information leaks.

Another key objective is to maintain the integrity of Stackle's data and IT resources. This involves implementing controls that prevent unauthorized modifications or tampering with the data, as well as ensuring that authorized users only modify data within the scope of their job responsibilities. Preserving data integrity is crucial for maintaining the accuracy and reliability of Stackle's online education technology services.

Moreover, this policy aims to ensure the availability of Stackle's information assets and systems by implementing measures that prevent unauthorized users from disrupting or overloading the systems, while also enabling authorized users to access the resources they need in a timely and efficient manner.

By focusing on the principles of confidentiality, integrity, and availability, this Access Control Policy helps Stackle maintain a strong security posture and build trust with its customers, partners, and stakeholders. The policy supports Stackle's commitment to delivering high-quality online education technology services while safeguarding the organization's valuable data and IT resources from potential security threats and incidents.

3. Scope

This policy applies to all Stackle employees, contractors, and third parties who access or interact with the company's information assets and systems.

4. Policy Statements

4.1. Role-Based Access Control (RBAC)

RBAC is an access control method that focuses on managing access rights based on predefined roles associated with specific job functions. The RBAC model ensures that users are granted access to resources only as required to fulfill their responsibilities, adhering to the principle of least privilege. Here are additional details for implementing RBAC in Stackle:

4.1.1. Role Definition

Roles should be clearly defined to represent specific job functions or responsibilities within Stackle. Examples of roles may include Administrator, Instructor, Content Developer, IT Support, Finance, HR, and Student. Each role should have a clear description outlining its associated duties and access requirements.

4.1.2. Access Rights Assignment

Once roles are defined, access rights should be assigned to each role, specifying the type of access (e.g., read, write, modify, delete) to relevant information assets and systems. Access rights should be documented in a role matrix, which maps each role to its corresponding access rights. This matrix should be reviewed and approved by both the user's manager and the IT department.

4.1.3. Role Hierarchies and Inheritance

Roles can be organized hierarchically to allow for inheritance of access rights, where a higher-level role inherits the rights of its subordinate roles. For example, a Manager role might inherit the access rights of an Employee role, in addition to having its own unique access rights. This approach simplifies the management of access rights and reduces the risk of granting excessive privileges.

4.1.4. Separation of Duties

Implementing the concept of separation of duties can further enhance security by ensuring that critical tasks or processes require the involvement of multiple individuals with different roles. This can

help prevent fraud, errors, or unauthorized access by making it more difficult for a single individual to carry out malicious actions.

4.1.5. Role Lifecycle Management

Roles should be subject to regular review and updates to ensure that they remain aligned with the organization's evolving needs and job functions. This includes adding new roles, modifying existing roles, or removing obsolete roles as necessary. Any changes to roles or their associated access rights should be documented, approved by appropriate stakeholders, and communicated to affected users.

4.1.6. Role Assignment to Users

Users should be assigned to roles based on their job functions and responsibilities. Role assignments must be authorized by the user's manager and approved by the IT department. Users may be assigned to multiple roles if required, but care should be taken to avoid conflicts of interest or excessive access rights.

4.2. User Access Requests

4.2.1. Access Request Submission

Users or their managers must submit access requests using a designated form or system, providing all necessary information, including the user's name, job title, department, required access rights, and a justification for the requested access. The form should also indicate whether the access request is for a new user, a change in access rights for an existing user, or a temporary access requirement.

4.2.2. Manager Authorization

The user's manager is responsible for reviewing the access request and confirming that the requested access rights are appropriate for the user's job function. If approved, the manager must authorize the request and forward it to the IT department for further processing.

4.2.3. IT Department Approval

The IT department is responsible for reviewing authorized access requests, ensuring they align with the principle of least privilege and comply with Stackle's security policies. The IT department may consult with other stakeholders, such as data owners or security officers, to determine the appropriateness of the requested access. If approved, the IT department will grant the access rights and inform the user and their manager.

4.2.4. Access Rights Review

Access rights must be reviewed periodically (e.g., annually or semi-annually) to ensure they remain appropriate for each user's job function. Managers, in collaboration with the IT department, should verify that users still require their assigned access rights and identify any necessary changes, such as revoking access rights that are no longer needed or granting additional rights due to a change in job responsibilities.

4.2.5. Temporary Access

In cases where users require temporary access to information assets or systems (e.g., for a specific project or a short-term assignment), the access request should specify the duration of the access requirement. Temporary access rights must be automatically revoked upon the specified end date, and the IT department should confirm the revocation with the user's manager.

4.3. Authentication

4.3.1. Unique Credentials

Users must authenticate themselves using unique credentials before accessing Stackle's information assets and systems. Each user is assigned a unique username and is responsible for creating and maintaining a secure password, as well as enabling and using multi-factor authentication (MFA) where available.

4.3.2. Password Requirements

Passwords must meet the following complexity and length requirements:

- At least 12 characters in length
- A combination of uppercase and lowercase letters, numbers, and special characters
- No use of easily guessable information (e.g., names, birthdates, or common phrases)
- No reuse of previous passwords within the last five password changes
- Users are required to change their passwords every 90 days, and the system will enforce these password requirements.

4.3.3. Multi-Factor Authentication (MFA)

Where possible, users are required to enable and use MFA, which adds an additional layer of security by requiring a second form of authentication (e.g., a one-time code sent via text message, email, or an authenticator app) in addition to the username and password. MFA must be used for accessing critical systems, remote access to the corporate network, and any other high-risk activities as determined by the IT department.

4.3.4. Credential Management

Users are responsible for managing and safeguarding their credentials, ensuring that they are not shared with others or written down where they may be easily discovered. Users must immediately report any suspected compromise of their credentials to the IT department, who will initiate the process to reset the affected credentials.

4.3.5. System Lockouts and Account Suspensions

To protect against unauthorized access attempts, the system will enforce a lockout policy after a specified number of consecutive failed login attempts (e.g., five attempts). Accounts will be temporarily locked for a specified period (e.g., 30 minutes), after

which the user can attempt to log in again. If an account is locked due to multiple failed login attempts, users are encouraged to report the incident to the IT department to investigate potential security threats.

4.4. Access Review and Monitoring

4.4.1. Access Review Process

Regular access reviews will be conducted at least semi-annually or as required by any significant organizational changes. The access review process will involve the following steps:

- IT department generates access reports for all users, detailing their current access rights and roles.
- Managers review access reports for their respective teams, ensuring that users have appropriate access levels based on their job functions.
- Managers identify any unnecessary or inappropriate access rights and submit requests for modification or removal to the IT department.
- IT department processes the requests, updates the access rights, and maintains a record of changes for audit purposes.
- IT department verifies that changes have been implemented correctly and notifies the managers of the completion of the access review process.

4.4.2. Logging and Monitoring

User access to information assets and systems will be logged and monitored to detect and respond to potential security incidents or policy violations. This process includes:

- Implementing logging mechanisms to record user access, including successful and unsuccessful authentication attempts, data access, and modification activities.

- Using monitoring tools to analyze access logs for unusual or suspicious activity, such as multiple failed login attempts, unauthorized access attempts, or access outside of normal working hours.
- Configuring alerts and notifications to inform the IT department of potential security incidents or policy violations detected through log analysis.
- Investigating alerts and notifications to determine the cause of the incident, assess its impact, and initiate appropriate response actions.

4.4.3. Reporting and Incident Response

If the monitoring process identifies a potential security incident or policy violation, the IT department will:

- Notify relevant stakeholders, including affected users, managers, and the executive team, depending on the severity and impact of the incident.
- Initiate the Incident Response Plan to mitigate risks, investigate the cause, and take appropriate action to prevent future occurrences.
- Document the incident, including a description of the event, its impact, the response actions taken, and any lessons learned or recommendations for policy updates or process improvements.
- Conduct a post-incident review to evaluate the effectiveness of the response actions and identify opportunities for enhancing the Access Control Policy or monitoring processes.

4.5. Access Termination

4.5.1. Employee Termination Procedure

When an employee leaves the company, either voluntarily or involuntarily, the HR department must inform the IT department and

the employee's manager immediately. The IT department is responsible for promptly revoking all access rights, disabling the user's account, and deactivating any physical access tokens (e.g., access cards, key fobs) the employee may possess.

4.5.2. Employee Role Change Procedure

In cases where an employee's job responsibilities change, the employee's manager must assess the new role and determine the appropriate access rights. The manager must then submit a formal request to the IT department for access modification. The IT department must verify the new access rights align with the principle of least privilege and promptly modify the user's access accordingly.

4.5.3. Temporary Access Suspension

If an employee goes on extended leave (e.g., medical, parental, or sabbatical leave), their access rights should be temporarily suspended to reduce the risk of unauthorized access during their absence. The employee's manager must inform the IT department of the leave dates, and the IT department will reactivate the user's access upon their return, provided that the access rights remain appropriate for their job function.

4.5.4. Access Termination Checklist

The IT department must maintain an access termination checklist to ensure that all necessary steps are taken during the access termination process. This checklist should include:

- Disabling user accounts on all relevant systems and applications
- Revoking access to shared resources (e.g., file servers, databases)
- Deactivating physical access tokens (e.g., access cards, key fobs)
- Revoking remote access and VPN privileges

- Removing the user from email distribution lists and communication platforms
- Archiving and transferring the user's data as needed (e.g., files, emails)
- Reclaiming company-issued devices and equipment

4.6. Third-Party Access

4.6.1. Third-Party Risk Assessment

Before granting third-party access to Stackle's information assets and systems, a risk assessment must be conducted to evaluate the potential risks associated with the third party's access. This assessment should consider the third party's security practices, track record, and potential impact on Stackle's security posture.

4.6.2. Third-Party Agreement

Third parties must sign a formal agreement outlining their responsibilities, access rights, and obligations to comply with Stackle's security policies and procedures. This agreement should include clauses related to data protection, confidentiality, incident reporting, and the right for Stackle to audit the third party's compliance with the agreement.

4.6.3. Access Control for Third Parties

Third-party access should be granted on a need-to-know basis, following the principle of least privilege. Access rights should be limited to the specific information assets and systems necessary for the third party to perform their contracted services. User accounts for third parties must be uniquely identifiable and subject to the same authentication requirements as Stackle employees.

4.6.4. 3.6.4. Monitoring and Review

Third-party access to Stackle's information assets and systems should be monitored and logged to ensure compliance with the agreed-upon terms and detect potential security incidents. Regular

access reviews should be conducted to confirm that third-party access remains appropriate and necessary. Any changes to the third party's scope of work or personnel should be promptly reflected in their access rights.

4.6.5. Termination of Third-Party Access

Upon the completion of the contracted services or termination of the agreement, third-party access to Stackle's information assets and systems must be promptly revoked. A thorough review of the third party's activities during the period of access should be conducted to identify any potential security incidents or policy violations.

4.6.6. Incident Response Involving Third Parties

In the event of a security incident involving a third party, Stackle's Incident Response Plan must be followed, with the third party expected to cooperate fully in the investigation and remediation process. The third party must report any security incidents involving Stackle's information assets and systems as soon as they are identified.

5. Policy Enforcement

Violations of this Access Control Policy may result in disciplinary action, up to and including termination of employment or legal action. All users are responsible for reporting any suspected policy violations or security incidents to the IT department.

6. Policy Review and Updates

This policy will be reviewed and updated periodically to ensure its continued effectiveness and alignment with Stackle's evolving business needs and the online education technology landscape. Users will be notified of any significant policy changes or updates.

7. Training and Awareness

All Stackle employees, contractors, and third parties with access to information assets and systems must undergo security awareness training, including the principles outlined in this Access Control Policy. Refresher training will be provided periodically to ensure that users maintain an up-to-date understanding of access control requirements and best practices.

8. Incident Response

The Incident Response Plan (IRP) is a critical component of Stackle's security program, outlining the processes and procedures for managing security incidents involving unauthorized access to information assets or systems. The goal of the IRP is to minimize the impact of security incidents, protect Stackle's resources, and maintain the trust of customers and stakeholders.

8.1. Incident Detection and Reporting

Early detection of security incidents is crucial for effective incident response. Users, automated monitoring tools, or third-party partners may identify potential incidents. Users must immediately report any suspected security incidents or access control policy violations to the IT department or designated security personnel.

8.2. Incident Assessment and Triage

Upon receiving a security incident report, the IT department will assess the situation to determine the scope, severity, and potential impact of the incident. They will classify the incident according to its criticality and assign it to the appropriate incident response team members for further investigation and action.

8.3. Incident Containment

Once an incident has been identified and assessed, the incident response team will work to contain the threat and limit any potential damage. This may involve isolating affected systems, revoking user access, or

implementing additional security measures to prevent further unauthorized access.

8.4. Incident Eradication

After containing the incident, the incident response team will identify and eradicate the root cause of the security breach. This may involve removing malicious software, patching vulnerabilities, or addressing weaknesses in access control policies and procedures.

8.5. Recovery and Restoration

Following the eradication of the threat, the incident response team will work to restore affected systems and data to their normal state. This may involve data restoration from backups, system repairs, or the implementation of additional security measures to prevent similar incidents in the future.

8.6. Post-Incident Analysis and Lessons Learned

Once the incident has been resolved, the incident response team will conduct a post-incident analysis to determine the effectiveness of the response, identify any gaps in the incident response process, and learn from the event. The analysis will inform updates to the IRP, access control policies, and security awareness training to enhance Stackle's overall security posture.

9. Auditing and Compliance

Regular audits will be conducted to assess compliance with this Access Control Policy and identify any potential gaps or weaknesses in access control processes. Audit findings will be used to inform policy updates, process improvements, and targeted training to enhance Stackle's overall security posture.

10. Exceptions

Any exceptions to this Access Control Policy must be documented and approved by both the user's manager and the IT department. Exceptions will be granted on a case-by-case basis and will be subject to periodic review to ensure their continued appropriateness.

11. Responsibilities

All Stackle users are responsible for complying with this Access Control Policy and maintaining the security of their access credentials. Managers are responsible for authorizing and reviewing user access rights based on job functions, while the IT department is responsible for managing, monitoring, and enforcing access controls across the organization.