WHITEPAPER

How to Prevent **Payroll Fraud and Security Breaches**

10:38

Browse and Select Security Profile

Search

1 of 1 6 Rows

	Name	Description
○	Applicant	This is a default security pr assigned to all applicants.
○	Company Administrator	Company Administrator -- A cess to all functions
○	Department Manager	Provides general system ac cess with ability to run basi reports
●	Employee	Limited access to time entr and accrual information
○	Paul Peterson Security Profile	Company Administrator -- A cess to all functions
○	Payroll Admin	Payroll Admin -- Access to a functions

10:16

◂ Search

inova

Configure Virtual Code Settings

Please select one of the following methods to validate identity. A code will be sent to the method chosen.

You will need to enter this code after you receive it. It should only take a moment to receive it once you've m your selection.

Methods:

○ Text Message

○ Voice

● Email

Email will be sent to: l******n@inovapayr

Enter Code*

Innovation Pays

$45,000

That's the median loss US businesses face from payroll fraud.

You may think that it can never happen to you. You trust your employees to do right by you and your business.

That's great. But even if you're certain you're safe from internal malice, human error can expose your payroll data to external threats. In fact, almost 85% of executives believe that employee negligence is the biggest risk to information security.

The worst part: In some payroll fraud and security breach cases, it may be too late before you realize what's happening!

All things considered, you simply can't be too careful when it comes to payroll security. Your only safe bet is to place strong security protocols and vigilantly monitor your payroll cycles. In this whitepaper, we'll share popular measures and tactics that you can start using today to make your payroll more secure.

Document Your Payroll Management Process

Perhaps one of the biggest security risks is an unclear process for running payroll and handling employee data. Without clear steps to follow, HR/ payroll personnel are more likely to make errors and expose your company's compensation data to a world of threats. It also sets you up for failure when a new employee joins the team and is not familiar with how payroll is typically handled.

So if you haven't already, document your company's payroll process and share it with the staff members responsible for handling payroll. The document should include the following essential information:

- The way timesheet data is collected, analyzed, and processed (and by whom)
- Where and how the paychecks are calculated (and who manages them)
- Who approves the final paychecks
- How payments are made to the employees and through which channel(s)
- What steps to take when an employee complains about receiving lower pay than anticipated
- The standard operating procedure for when an employee doesn't receive their pay even when you process it

Remember: there's no such thing as a perfect business process. Revisit this document from time to time and see if there's any way you can make your payroll procedure more airtight.

Restrict Access to Payroll Data

Be very mindful of who can access your payroll system and employee data. The wrong person can manipulate time cards, authorize unearned bonuses/overtime, misuse confidential employee information, or divert paychecks to unknown bank accounts.

Only a select few people from HR who process paychecks should therefore have access to anything that's even remotely related to your payroll. The goal is to only have it managed by the personnel who have received training in this area.

To limit payroll access, consider following the **Separation of Duties (SoD)** principle. In this context, SoD would entail splitting payroll duties across multiple team members. A single person who oversees the payroll process end-to-end is likely to make mistakes. Plus, you shouldn't give one person that much control and privilege.

SoD helps minimize errors and distribute power across the HR team. You could have one person manage time data, another run the payroll, and a third issue the checks. With this system, every person involved in payroll is less likely to misuse their authority since they'll know that other people are closely monitoring their activity. And with a solution like the Inova HCM, you can create custom profiles for different employees with varying levels of privileges (depending on their seniority and relevance to payroll).

In addition to separating duties, **run extensive background checks** that comply with the Fair Credit Reporting Act on any new employees you hire (with the help of a trustworthy service). Specifically, tap into their criminal records to ensure that they don't have any convictions for financial-related offenses.

Encrypt Your Payroll Data

Keep your payroll data safe by encrypting it — converting it into a secret code so outsiders can't decipher the information. Encrypted information appears like visual gibberish — a collection of random characters, letters, and numbers that don't make sense. It can be "decrypted" into meaningful information by authorized personnel using a software.

Even if your company's encrypted payroll data falls into the wrong hands, it's pretty much useless until it's decrypted. Speak to your payroll software vendor (or internal tech support if you use a native program) to see if they can offer encryption protocols.

Encourage Employees to Change Their Passwords Frequently

Hackers are less likely to gain access to your payroll data and system if passwords are regularly updated. To this end, have your employees regularly update their login credentials. You might think that only large businesses need their employees to regularly update their passwords since they're more likely to become targets of cyberattacks. This is far from the truth — small businesses are just as susceptible, if not more, to cyber threats. So make sure to follow this tip, regardless of your payroll size!

And if you haven't already, secure your payroll system with multi-factor authentication (MFA), too. This protocol adds an extra layer of security by requiring employees to prove their identities through an additional step.

MFA typically requires you to provide a code sent to your email, phone number, or another connected application where you're signed in. Only then are you able to access your system and make any changes (such as updating your password).

Regularly Update Your Payroll Software

As hackers get smarter, payroll software vendors frequently roll out new updates with improved security features to keep up. A modern solution, like the Inova HCM, handles all updates automatically, so you don't have to do anything on your end. However, in case the product you currently use doesn't do that, make sure to regularly update the desktop and/or mobile application on your end to protect your business from new security threats.

If your payroll software has a mobile application, instruct everyone to update whenever a new patch is released.

Offboard Employees Properly

Employees who have left your organization but can still access their payroll reports (or worse, the entire system) pose a huge threat to your payroll security. Ex-personnel may misuse existing employees' payroll information, embezzle your organization's money, or even continue to receive paychecks if they don't receive proper offboarding.

To this end, make sure that you follow this offboarding checklist whenever an employee quits:

- ☑ **Remove them from the active list of employees** on your payroll software. Update your system to ensure they don't receive another full paycheck (unless you owe them).
- ☑ **Delete their account from your payroll system.** Ensure their credentials no longer work, especially if they had administrative privileges.
- ☑ **Retrieve any company-issued laptop or mobile phone from them** since it might have payroll records and other sensitive information of your employees.
- ☑ **Make sure not to delete their records right away** to comply with the Fair Labor Standards Act (FLSA). You're required to keep payroll records for at least 3 years for reporting purposes. A payroll system with multi-year history tracking and reporting — such as Inova HCM — makes it easier to comply with this requirement!

Use a Reliable Time and Attendance System

Time theft is a common type of payroll fraud where an employee reports more hours than they actually worked in a period to receive a higher (unjustified) paycheck. It's difficult to detect this theft if you still use a manual process or an outdated software that makes it easy to manipulate data.

If your payroll system is outdated or manual, switch to a reliable time and attendance software with modern features that prevent time theft. Inova HCM gives you the option to verify the identity of the person adding their time with systems like biometric, proximity, and barcode readers. It also lets you set custom rules to limit where and when employees can clock in and out.

Frequently Run Payroll Audits

A payroll audit is a great way to not only guarantee that you're complying with the law but also ensure you're not a victim of any fraudulent activity. These audits can be conducted either by an in-house professional or by an outside consultant. A good practice is to run them once every quarter or twice a year to catch and rectify any discrepancies before it's too late.

As far as preventing payroll fraud and security breaches goes, here's what your audit checklist should include:

- ☑ Check to see if the payroll process laid out by your business is being followed to a T or not. All team members should be performing their assigned duties as instructed.
- ☑ Review the list of employees with admin privileges in your payroll system. Make sure that the profiles/accounts of any ex-employees are no longer active.
- ☑ Compare your list of active employees with those in the payroll. If someone is on the latter but not the former, chances are that they're a "ghost employee." This is a common type of payroll fraud where a staff member embezzles money by paying an entity that doesn't work for your company.
- ☑ Review the list of the people currently on your payroll to ensure there's no ex-employee who is still receiving paychecks.
- ☑ Cross-check the hours of your employees recorded in your time and attendance software with your payroll records.
- ☑ Check the bonuses, commissions, and any other form of additional compensation paid to your employees. All extra pay should have been approved by the relevant authority.
- ☑ Review any off-cycle payroll throughout the quarter/year to ensure it was authorized. If you see records of any off-cycle payroll, ask your staff/partner for a detailed report on the reason(s) that prompted it.

A GOOD TIP

is to conduct these audits unannounced and at irregular intervals. That way, if by any chance anyone is involved in embezzling your company's money, they won't get a chance to cover their tracks.

Train Your Employees on Payroll Security

Your first line of defense against payroll fraud is your employees, so it's critical that they receive ample training about security threats. Launch a company-wide, mandatory course that trains your employees on:

- The day-to-day use of their payroll systems and how to share sensitive company data (and when)
- How to protect the company from phishing, malware, and other common cyber threats
- How to identify and report potential payroll fraud
- The best way to respond to a security breach based on your disaster recovery and business continuity plans

Make it mandatory for all employees to retake the training course every year and update it frequently with new material. Along with annual payroll security training, hold regular workshops and tabletop exercises to simulate emergency situations.

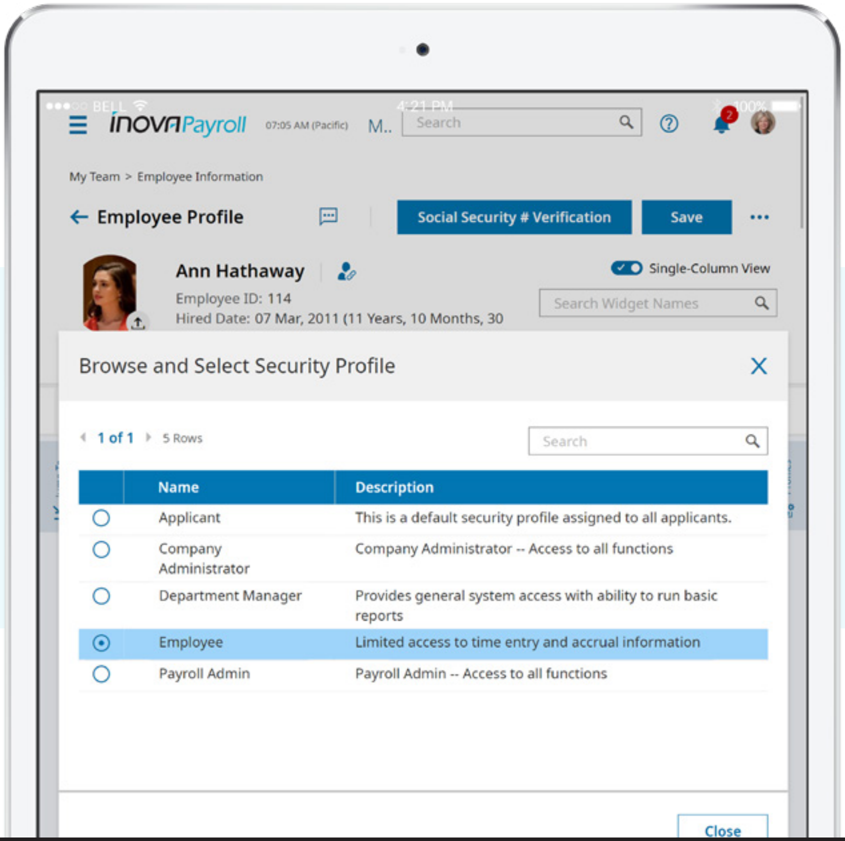
Protect Yourself from Payroll Fraud and Breaches with Inova!

Your payroll is one of your organization's most precious assets. But important as it is, constantly monitoring your payroll system for security threats can be exhausting.

Fortunately, working with a reliable payroll service provider will take away most challenges that comes with protecting your company's payroll.

If you're currently looking for a reliable payroll partner you can trust, consider Inova. We specialize in offering a personalized, white-glove payroll experience where you get much more than payroll processing. Our experts go the extra mile to provide all the support and care you need to succeed with a best-in-class payroll solution that offers the following features:

- **Open API** — exchange information securely and easily with other third-party platforms
- **Custom time tracking** — record hours through whatever medium or method that best suits your business
- **Payment flexibility** — pay your employees through channels that you're most comfortable using
- **Multi-factor authentication** — protect against fraud, data loss, and identity theft



My Team > Employee Information

Ann Hathaway
Employee ID: 114
Hired Date: 07 Mar, 2011 (11 Years, 10 Months, 30

Browse and Select Security Profile

1 of 1 5 Rows

	Name	Description
○	Applicant	This is a default security profile assigned to all applicants.
○	Company Administrator	Company Administrator -- Access to all functions
○	Department Manager	Provides general system access with ability to run basic reports
●	Employee	Limited access to time entry and accrual information
○	Payroll Admin	Payroll Admin -- Access to all functions

Ready to take your payroll security to the next level?

Request a demo